UNIVERSIDAD POLITECNICA SALESIANA

FACULTAD DE INGENIERÍAS

SEDE QUITO-CAMPUS SUR

CARRERA DE INGENIERÍA DE SISTEMAS

MENCIÓN TELEMÁTICA

AUDITORIA INFORMÁTICA DE LA SEGURIDAD DE LA RED FÍSICA Y LÓGICA PARA EL DEPARTAMENTO DE GESTIÓN INFORMÁTICA Y SISTEMAS DE LA DIRECCIÓN PROVINCIAL DE SALUD DE PICHINCHA (DPSP)

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS

SONIA ELIZABETH BUÑAY CALLE
EMILLY JEANETTE GUANOTUÑA LASCANO

DIRECTOR ING. RAFAEL JAYA

Quito, enero del 2009

DECLARACIÓN

Nosotras, Sonia Elizabeth Buñay Calle y Emilly Jeanette Guanotuña Lascano, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Politécnica Salesiana, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

---------- ----------

Egr. Sonia Buñay Calle Egr. Emilly Guanotuña Lascano

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Sonia Elizabeth Buñay Calle y Emilly Jeanette Guanotuña Lascano bajo mi dirección.

Director de tesis

AGRADECIMIENTOS

Agradezco a Dios por ayudarme en cada segundo de mi vida tanto a nivel profesional como personal, y sobretodo por el desarrollo de este Proyecto.

Como también mis más sinceros agradecimientos al Sr. Gonzalo Cevallos y Sra. Fanny Alcívar mis queridos suegros quienes me ayudaron en todos los momentos, no solo en el desarrollo de este proyecto, sino en cada instante de mi vida.

Sonia

Agradezco a Dios Todopoderoso por permitirme terminar esta etapa de mi vida, sin su ayuda todo esfuerzo hubiese sido en vano.

A mis padres por su apoyo incondicional y confianza brindada a lo largo de mi existencia.

A mis hermanos: Jorgito, Patricio y Diego por su amor y comprensión. A mi compañera de tesis y familia, por acogerme en su casa, y por el cariño brindado.

Al Ing. José Luis Torres Gerente de Macronet Cia. Ltda. quien con su profesionalismo y experiencia ha sabido brindarme conocimientos acertados los mismos reposan en este trabajo, y también por la confianza depositada al prestarme gentilmente los equipos para la certificación del cableado FLUKE DTX 1800 (UTP).

Emilly

Al Ing. Rafael Jaya quien confió en nosotras al darnos su apoyo a lo largo de esta tutoría, por sus guías para la culminación de este proyecto de manera satisfactoria.

Sonia y Emilly

DEDICATORIAS

Este proyecto de tesis lo dedico a lo más hermoso de mi vida, a mi hija Ruby que a pesar del tiempo que teníamos para estar juntas lo sacrifique, para culminar con esta meta, espero que este sea un estímulo para su vida profesional.

A mi amado esposo por su compresión y apoyo para lograr éste, mi objetivo que se convirtió de los dos.

A mis Padres por ser personas luchadoras y emprendedoras que me enseñaron el verdadero valor del progreso, a quienes los amo y agradezco por todas las cosas que hicieron y lo siguen haciendo por mí y mi familia.

Sonia

Dedico este proyecto de tesis a Dios quien es el autor principal de esta tesis, ya que es la fuente de toda sabiduría e inteligencia.

A mis padres por darme la oportunidad de estudiar, quienes no escatimaron nada, quienes han estado a mi lado a lo largo de estos años, prestos a darme una palabra de aliento cuando lo he necesitado.

A mis hermanos Jorgito, Patricio y Diego que todo sacrificio da frutos buenos y sea este trabajo un estimulo para concluir él de ellos.

Emilly

RESUMEN

En el siguiente resumen el lector concebirá una idea clara acerca del presente proyecto investigativo, denominado Auditoria Informática de la Seguridad de la Red Física y Lógica para el Departamento de Gestión Informática y Sistemas de la Dirección Provincial de Salud de Pichincha.

En el primer capítulo, el lector se encuentra frente a los Antecedentes más destacables de la Institución como son Situación Actual de la Dirección Provincial de Salud de Pichincha en lo referente a lo Tecnológico, y sobre todo la Situación Actual del Proceso de Gestión Informática en sus diferentes áreas, realizando un levantamiento de todas las falencias que se realizan con respecto a la Seguridad tanto Física como Lógica de la Red. Con esta información recopilada se pudo realizar el Planteamiento del Problema, Objetivo General & Específicos, Justificación, Alcance y la Descripción del Proyecto de la Auditoria.

En el segundo capítulo, se exhibe el análisis y evaluación de los riesgos tecnológicos a los que están expuestos los recursos informáticos en la Dirección Provincial de Salud de Pichincha, como también la identificación de amenazas y vulnerabilidades; el análisis y evaluación de los riesgos fue basada en el estándar NIST 800-30, para poder realizar la correcta evaluación de costos y así presentar las posibles medidas de protección.

En el tercer capítulo, se detalla el desarrollo y ejecución de la auditoria para la gestión de seguridad de la red física y lógica de la Dirección Provincial de Salud de Pichincha, metodología empleada, plan de trabajo realizado por el auditor, e informe preliminar de la auditoria realizada.

En el cuarto capítulo, se observa la elaboración y ejecución del instructivo a ser implementado en el Proceso de Gestión Informática de la Dirección Provincial de Salud de Pichincha, en el Cuarto de Servidores y los informes presentados de las principales Fases de la Metodología.

Finalmente el quinto capítulo, contiene Conclusiones y Recomendaciones

PRESENTACION

La presente Auditoria Informática, esta propuesta a la seguridad de la red física y lógica del Proceso de Gestión Informática de la Dirección Provincial de Salud de Pichincha.

Para el correspondiente análisis, se realizó un minucioso estudio del estado actual del Proceso, enfocándonos en las tres áreas mas importantes como son: área de hardware, área de software y área de comunicaciones, los cuales fueron examinados por medio de hallazgos de auditoria y formularios de visitas, como también basándonos en las herramientas de auditoria como son: entrevistas, cuestionarios y checklist

El análisis se concibió en las diferentes áreas ya citadas en el párrafo anterior con ayuda de herramientas y software que ayudaron a identificar las vulnerabilidades y las amenazas a las que la Seguridad Informática del Proceso de Gestión Informática están expuestas, luego de la identificación se realizó el debido y acertado análisis de riegos basado según el estándar NIST 800-30, el mismo que ayudó a analizar los riesgos y a cuantificar los costos, mediante ecuaciones y matrices, obteniendo una breve identificación de los recursos más importantes para el Proceso y la Institución, de acuerdo al trato que este Proceso realiza a cada uno de los recursos informáticos, obteniendo las diferentes falencias y generando sus debidas recomendaciones, basadas en la norma ISO/IEC 17799:2007 “Código de Buenas Prácticas para la Gestión de la Seguridad de la Información”. Sobre la cual fue basada la generación de un enfocado instructivo de procedimientos para el Cuarto de Servidores del Proceso de Gestión Informática.

CONTENIDO

Índice de Figuras: Página

Índice de Tablas: Página

CAPITULO I

1 ANTECEDENTES

1.1 SITUACIÓN ACTUAL

1.1.1 VISIÓN

El Ministerio de Salud Pública asegurará el acceso universal y solidario a servicios de salud con atención integral de calidad para todas las persona, familias y comunidades, especialmente a las de condiciones más vulnerables, para garantizar una población y ambientes saludables consolidando su rectoría en el sector e impulsando la participación de la comunidad y del personal de salud en la formulación y ampliaciones concentrada y descentralizada de las políticas sanitarias

1.1.2 MISIÓN

Velar por el cumplimiento del principio consagrado en la Constitución Política, a la cual el estado garantiza el derecho irrenunciable a la salud, su promoción y protección incorporando practicas de medicinas tradicionales y alternativas, involucrando a todos los sectores y actores responsables en los ámbitos nacionales, provincial y local mediante la organización y funcionamiento del Sistema Nacional de Salud de manera desconcentrada, descentralizada y participativa , cumpliendo con los principios de equidad, integridad, solidaridad, universalidad, participación, pluralidad, calidad y eficiencia.

1.1.3 DESCRIPCIÓN DE LA ORGANIZACIÓN ADMINISTRATIVA DE LA DIRECCIÓN PROVINCIAL DE SALUD DE PICHINCHA (DPSP)

La Dirección Provincial de Salud de Pichincha, es una institución Pública que se encarga de controlar y mantener un buen sistema de salubridad en todos los establecimientos públicos y privados de acuerdos a reglamentos y ordenamientos estipulados por el Ministerio de Salud de Pichincha.

Esta institución esta organizada por procesos que son los diferentes Departamentos, cada proceso tiene un responsable al que le denominan coordinador del proceso y siendo su autoridad máxima la Dirección.
Cada proceso tiene su función específica para cada necesidad y/o control hacia la comunidad en los diferentes ámbitos o campos que intervenga la Salubridad, como son:

- Estadística
- Redes de Salud
- Subdirección Técnica
- Jurídico
- Salud Integral
- Salud Intercultural
- Informática
- Infraestructura Física
- Salud y medio Ambiente
- Control y Vigilancia Sanitaria
- Epidemiología
- Comisaría
- Servicios Institucionales
- Tesorería
- Financiero
- Riesgos y Desastres
- Secretaria general
- Comunicación
- Recurso Humanos
- Farmacia

1.1.4 DESCRIPCIÓN DEL PROCESO DE GESTIÓN INFORMÁTICA (PGI)

El Proceso de Gestión Informática, es un proceso habilitante de apoyo que es responsable del diseño, desarrollo y operación de los sistemas informáticos, incluyendo análisis y especificación de requisitos, diseño técnico, dirección de

proyectos informáticos, apoyo técnicos y administración de sistemas, datos, redes de comunicaciones y seguridades, adaptando a una estructura piramidal de la informática.

Con la misión de integración y coordinación general de los servicios informáticos, cuyas actividades se relacionan en cuatro campos con fines más específicos relativos a: Equipamiento, Redes, Comunicaciones y Aplicaciones.

1.1.4.1 Misión

Administrar en forma eficiente y eficaz de los recursos computacionales, informáticos de comunicaciones e implementación de nuevas tecnologías a fin de mejorar la disponibilidad de información a través de aplicaciones, apoyo técnico, soporte, difusión y capacitación a todos los usuarios de la DPSP, Áreas de Salud y Hospitales, con agilidad, eficacia, tecnología de punta, responsabilidad y trasparencia de manera que contribuyan a perfeccionar los procesos operacionales y requerimientos de los usuarios internos y externos de la Red de Servicios de Salud de la DPSP y elevar el nivel técnico y operativo del hardware y software existentes.

1.1.4.2 Objetivos

El Proceso de Gestión Informática de la DPSP, se enmarca dentro de los que es la definición de la misión del Proceso de Gestión Informática y la visión de lo que debería ser este soporte en un plazo de cinco años.
La misión del Proceso de Gestión Informática de la DPSP, se definió y tiene el siguiente planteamiento:
“Administrar en forma eficiente y eficaz de los recursos computacionales, informáticos de comunicaciones e implementación de nuevas tecnologías a fin de mejorar la disponibilidad de información a través de aplicaciones, apoyo técnico, soporte, difusión y capacitación a todos los usuarios de la DPSP, Áreas de Salud y Hospitales, con agilidad, eficacia, tecnología de punta, responsabilidad y trasparencia de manera que contribuyan a perfeccionar los procesos

operacionales y requerimientos de los usuarios internos y externos de la Red de Servicios de Salud de la DPSP y elevar el nivel técnico y operativo del hardware y software existentes".

1.1.4.3 Objetivo General del Proceso de Gestión Informática (PGI):

Lograr que la DPSP sea una entidad cuya gestión este basada en un adecuado soporte de tecnología de información costo-efectivas, que apoye los procesos de producción con información adecuada, confiable y oportuna y que se vincule afectivamente con su entorno aprovechando las posibilidades que brindan estas tecnologías.

1.1.4.4 Objetivos Específicos del Proceso de Gestión Informática (PGI):

- Asegurar la integración y operaciones eficientes de la plataforma de sistemas de información que soportan los distintos procesos.
- Consolidar y continuar modernizando la plataforma tecnológica de la DPSP, asegurando la actualización permanente de su infraestructura y aprovechamiento de las oportunidades que plantea la innovación en materia informática.
- Conseguir la confiabilidad, oportunidad y seguridad de la información.
- Asegurar el perfeccionamiento continuo del personal en todas las áreas de conocimiento asociadas al trabajo en tecnologías de información.
- Transformar la relación entre informática y los diferentes Procesos de la DPSP para desarrollar un concepto de servicio al usuario basado en las necesidades y problemas del trabajo diario.

1.1.5 SITUACIÓN ACTUAL DEL PROCESO DE GESTIÓN INFORMÁTICA (PGI)

La Dirección Provincial de Salud de Pichincha (DPSP), es una Institución Pública que no ha tenido una organización definida en el control de la Seguridad de la red, tanto: en la seguridad física ya que no existe una intervención en la protección del hardware y de los soportes de datos; como en seguridad lógica que no se cuenta con la protección de los datos, procesos y programas, provocando muchos inconvenientes como: pérdidas de información, desconexión

de los equipos de computo hacia la red inalámbrica en reiteradas ocasiones por virus, como también el ingreso de diferentes amenazas accidentales: terremotos, inundaciones, influencias Electromagnéticas nocivas, errores de utilización, negligencia del personal, fallo del suministro eléctrico, averías del hardware, fallo del Software, delito contra intimidad, etc.; y/o amenazas intencionales: robo, fraude, utilización abusiva del computador, uso no autorizado de la información, etc.

El Departamento de Gestión Informática y Sistemas de la DPSP, esta consiente de todas esta eventualidades y es por eso que se ve en la necesidad de la obtención de un conjunto de procedimientos y técnicas para evaluar, controlar total o parcialmente los Sistemas Informáticos de esta institución, con el fin de proteger sus activos y recursos, verificando así si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática, para conseguir la eficacia exigida en el marco de la organización correspondiente.

El Departamento de Gestión Informática y Sistemas de la Dirección Provincial de Salud de Pichincha está en una etapa de evolución y mejoramiento en sus servicios, es por eso que se ve en la necesidad de encontrar y enfocar estrategias de seguridad para: las instalaciones, tecnología y sistemas de aplicación & datos, porque estas se encuentran vulnerables o están mal procedidas. A continuación se detallan algunas razones por lo cual es necesaria una auditoria informática:

- No se tiene un buen diseño de la red, encontrándose mal distribuidos los puntos de la misma, sin preveer el crecimiento de usuarios.
- El servidor de la red se encuentra saturado, tiene poca capacidad de almacenamiento en disco y de memoria, por lo tanto el acceso a la red es lento y además es portador de un sin número de virus, ya por su poca capacidad de almacenamiento y de recurso se dificultad la instalación de antivirus provocando así la propagación de virus y todo tipo de software maliciosos a nivel global de la red, sea esta inalámbrica o cableada.
- El antivirus que se tiene en los equipos de los usuarios, no es el más indicado, puesto que, este antivirus consume mucho recurso del computador.

- Por otro lado, no todos los computadores tienen esta herramienta, porque existe un limitado número de licencias provocando así un desbalance en el proceso de control de los virus.
- El estado actual en que se encuentran los servidores es preocupante, no teniendo ninguno de éstos un antivirus, hallándose la información vulnerable ante cualquier tipo de amenazas de índole informática.
- Los equipos que se encuentran conectados a la red inalámbrica, siempre se desconectan de la misma, causando molestias a los usuarios al momento de utilizar los recursos informáticos como: impresoras, Internet, Sistemas de uso internos que se encuentran en un ambiente de red.
- No existen políticas de distribución de la Banda Ancha.
- Los Access Point, no se encuentran en lugares apropiados provocando esto la Pérdida de la señal y siendo fácil de extraerlos.
- Actualmente no cuentan con una distribución de áreas, el personal técnico atiende toda inquietud o problemas informáticos que se presentan en la DPSP.

Se ha podido observar las diferentes funciones que manejan en el proceso de sistemas y se las ha separado de la siguiente manera:

1.1.5.1 Área Hardware[1]:

- Este proceso no cuenta con un parque informático, lo cual, genera muchos inconvenientes al momento de establecer decisiones en la adquisición de nuevos equipos, por lo tanto no se cuenta con un registro en el que se puede constatar que equipos necesitan mantenimiento preventivo, ni mucho menos saber en que estado se encuentran, al no tener esto no se puede contar con un control de garantías ni bajas de equipo (por deterioro).
- Actualmente, no se conoce el número exacto de equipos con los que cuenta la DPSP, pero se estima que cuenta con aproximadamente 230 equipos (desktop y laptops), y 7 servidores físicos y 2 virtuales.
- No existen puntos eléctricos suficientes para los equipos, ya que el número de funcionarios aumentado de los últimos años, es por eso que se ha

[1] Anexo 1. Resumen de inventario de hardware de algunos Servidores y Equipos de usuarios.

decidido poner varias extensiones eléctricas en cada proceso los cuales quedan en el paso de los usuarios, provocando así que se apaguen los equipos, corriendo con el peligro que estos tengan algún desperfecto.

1.1.5.2 Área Software[2]:

En lo referente al software la DPSP, cuenta con aplicaciones que se encuentran implementadas en varios servidores, sistemas que han sido adquirido en años anteriores por la DPSP y otros ofrecidos por el Ministerio de Salud, como también existe aplicaciones dispersas en diferentes Departamentos, sin que estos sean entregados al proceso de informática, sino que solo están instalados en los computadores del usuarios que necesitan dicha aplicación.

Actualmente el (PGI) cuenta con las siguientes aplicaciones:

- **Sistemas Informáticos:**

NOMBRE	PARA EL PROCESO DE:	DESARROLLADO EN:	BASE DE DATOS
GESTOR (ERP)	FARMACIA	ORACLE6I	ORACLE 9I
VGSIPF	CONTROL Y VIGILANCIA SANITARIA	VISUAL BASIC	SQL SERVER
SISPROD	ESTADISTICA	VISUAL FOXPRO	MYSQL
SGM	AREAS DE SALUD(5, 6 Y 8)	VISUAL BASIC	MYSQL
ANGEL	AREAS DE SALUD (9,2,13 Y 8)	JAVA	MYSQL
SIGEF	FINANCIERO	POWER BUILDER	ORACLE

[2] Anexo 2. Resumen de inventario de Software de algunos Servidores y Equipos de usuarios.

CONTROL DE CORRESPONDENCIA	SECRETARIA GENERAL	. NET	MYSQL
TRANSPORTES	CONTROL Y VIGILANCIA SANITARIA	. NET	MYSQL

Tabla 1. Sistemas Informáticos implementados

- **Herramientas Informáticas:**

NOMBRE	PARA EL PROCESO DE:	DESCRIPCIÓN
LEXIS	JURÍDICO	HERRAMIENTA DE BÚSQUEDA DE DOCUMENTOS LEGALES Y REGISTROS OFICIALES
NET SOPPORT	INFORMÁTICA (HACIA TODOS LOS USUARIOS)	HERRAMIENTA PARA SOPORTE REMOTO
CITRIX	FARMACIA SUR	HERRAMIENTA DE CONEXIÓN REMOTA
PANDA	EL 50% DE LOS USUARIOS	CONSOLAS DE ANTIVIRUS

Tabla 2. Herramientas Informáticas

- **Sistemas Operativos**

NOMBRE		INSTALADO EN:
Windows 2000	SERVICE PACK 4	DESKTOP- Usuarios
Windows XP	SERVICE PACK 2	DESKTOP- Usuarios

Windows Vista	-	DESKTOP- Usuarios
Windows 2000 Server	SERVICE PACK 2	SERVIDORES
Windows 2003 Server	-	SERVIDORES
Linux CentOS 10.0	-	SERVIDOR

Tabla 3. Sistemas Operativos

- **Utilitarios más usados:**

NOMBRE
ADOBE READER
OFFICE 2000,2003,2007 OPENOFFICE
WINZIP
WINRAR
WINDOWS MEDIA PLAYER
NERO
MESSENGER

Tabla 4. Utilitarios más usados

1.1.5.3 Área De Comunicaciones:

La DPSP cuenta actualmente con dos dominios de red:

1. DPSPSYS
2. PICDPSP

Las Direcciones de IP para la red del Dominio PICDPSP están distribuidas de la siguiente manera: Ver Tabla Nº. 5.

- **DPSP:**

IP	ASIGNACIÓN
10.64.32.1	Antena de Enlace de Interconexión
10.64.32.2/50	Servidores, Equipos de Interconexión e Impresoras de Red.
10.64.32.51	Puerta de Enlace o Gateway
10.64.32.52/254	Usuarios
10.64.33.1/254	Usuarios Red Inalámbrica

Tabla 5. Asignación de IP's Dominio PICDPSP

- **Áreas de Salud:**

  A las áreas de Salud se han otorgado las IP's de acuerdo a su número de área, Indicados: Ver Tabla Nº. 6.

ÁREA	IP	ASIGNACIÓN
AREA Nº. 01 Centro Histórico	10.1.0.1	Antena de Enlace de Interconexión
AREA Nº. 02 Las Casas	10.2.0.1	Antena de Enlace de Interconexión
AREA Nº. 03 La Tola	10.3.0.1	Antena de Enlace de Interconexión
AREA Nº. 04 Chimbacalle	10.4.0.1	Antena de Enlace de Interconexión
AREA Nº. 05 La Magdalena	10.5.0.1	Antena de Enlace de Interconexión
AREA Nº. 06 La Libertad	10.6.0.1	Antena de Enlace de Interconexión
AREA Nº. 07 Eplicachima	10.7.0.1	Antena de Enlace de Interconexión
AREA Nº. 08 Cotocollao	10.8.0.1	Antena de Enlace de Interconexión
AREA Nº.09 Comité del Pueblo	10.9.0.1	Antena de Enlace de Interconexión
AREA Nº. 10 San Carlos	10.10.0.1	Antena de Enlace de

		Interconexión
AREA Nº. 11 Pedro Vicente M Maldonado	10.11.0.1	Antena de Enlace de Interconexión
AREA Nº. 12 Cayambe	10.12.0.1	Antena de Enlace de Interconexión
AREA Nº. 13 Tabacundo	10.13.0.1	Antena de Enlace de Interconexión
AREA Nº. 14 Yaruqui	10.14.0.1	Antena de Enlace de Interconexión
AREA Nº. 15 Sangolquí	10.15.0.1	Antena de Enlace de Interconexión
AREA Nº. 16 Machachi	10.16.0.1	Antena de Enlace de Interconexión
AREA Nº. 17 Santo Domingo	10.17.0.1	Antena de Enlace de Interconexión
AREA Nº. 18 Nanegalito	10.18.0.1	Antena de Enlace de Interconexión
AREA Nº. 19 Guamani	10.19.0.1	Antena de Enlace de Interconexión
AREA Nº. 20 Chillogallo	10.20.0.1	Antena de Enlace de Interconexión
AREA Nº. 21 Calderón	10.21.0.1	Antena de Enlace de Interconexión
AREA Nº. 22 Los Rosales	10.22.0.1	Antena de Enlace de Interconexión
AREA Nº. 23 La Concordia	10.23.0.1	Antena de Enlace de Interconexión
AREA Nº. 24 Conocoto	10.24.0.1	Antena de Enlace de Interconexión

Tabla 6. Asignación de IP's para Áreas de Salud

- **Farmacia Sucursal Sur:**

IP	ASIGNACIÓN
10.64.64.1	Antena de Enlace de Interconexión
10.64.64.20/22/23	Usuarios

Tabla 7. Asignación de IP's Farmacia Sucursal Sur

Direcciones de IP para la red del dominio DPSPSYS están distribuidas de la siguiente manera:

IP	ASIGNACIÓN
10.64.34.1	IP del servidor en el que se encuentra configurado del Active Directory del Dominio DPSPSYS.
10.64.34.2/50	Servidores, Equipos de Interconexión e Impresoras de Red.
10.64.34.51/254	Usuarios

Tabla 8. Asignación de IP's Dominio DPSPSYS

Cabe indicar que entre los servidores, están establecidas las relaciones de confianza para su debida autentificación.

Las estaciones, se encuentran conectadas mediante una red hibrida, es decir, red inalámbrica y cableada de acuerdo al lugar en el que los equipos se encuentren.

En el caso de las redes inalámbricas no existen repetidoras de señal, lo cual provocan que algunas máquinas, tengan pérdidas de la señal constantemente ya que se encuentran lejanas de los Access Point.

En el caso de la red cableada, no existen los suficientes puntos de datos necesarios para los usuarios.

La topología que utilizan, es Estrella, con tecnología Fast Ethernet y Protocolo TCP/IP. Además cuentan con dos tipos de enlace de interconexión entre la DPSP y las áreas de salud:

1. Enlace de Datos: 6 Mb

2. Enlace de Internet:

- Enlace Dedicado-Abierto(sin ningún tipo de restricción o firewall) 512/256kbps, este canal es de uso exclusivo para el Proceso Financiero;
- Enlace Dedicado-controlado 1024/512kbps, este enlace se encuentra administrado en un servidor con un Sistema Operativo Linux, con la herramienta Squid la cual permite restringir el acceso a ciertos sitios, como también, esta herramienta permite administrar las cuentas de correo tanto de los usuarios locales como de las Áreas de Salud.

El Proveedor de éste enlace, es la empresa Punto Net, el cual proporciona la comunicación mediante un enlace de radio, esta empresa brinda soporte técnico cuando existen Pérdidas de señal tanto a la DPSP como a las áreas de salud, pero el soporte se realiza entre los técnicos de Punto Net y los técnicos de la DPSP mas no con técnicos de las aéreas, cuando estas tienen problemas con el enlace, esta acción hace que sea un trabajo centralizado y se evite descoordinación y/o duplicidad de actividades.

EQUIPO	MARCA	MODELO	DESCRIPCIÓN
ROUTER	CISCO	1700	VPN
ROUTER	CISCO	1700	INTERNET/eSIGEF
ROUTER	CISCO	1600	DATOS E INTERNET
ACCESS POINT	LINKSYS	WIRELESS-G	RED INALÁMBRICA
HUB	ACERHUB	116/16 PUERTOS	LAN
HUB	CISCO	24 PUERTOS	LAN
HUB	CISCO	24 PUERTOS	LAN
SWITCH	LINKS	48 PUERTOS	LAN
SWITCH	LINKS	48 PUERTOS	LAN
SWITCH	DLINK	DES-3226L	DATACENTER
SWITCH	ETHERNET SWITCH	24 PUERTOS	LAN

Tabla 9. Listado de Equipos de Comunicación

1.1.5.4 Topología Física de la red actual

En la siguiente figura se muestra el esquema de la Red Lan que la DPSP mantiene:

SE ADJUNTA ARCHIVO

Figura 1. Topología Física de la red de la DPSP

1.1.5.5 Topología Lógica de la red actual

La siguiente figura muestra la Topología Lógica de la red WLan y la distribución de los enlaces de datos e Internet que la DPSP mantiene:

SE ADJUNTA ARCHIVO

Figura 2. Topología Lógica de la red de la DPSP

1.1.5.6 Espacio Físico

En lo referente al área física del Proceso de Gestión Informática, el espacio no es el más apropiado, ya que el espacio físico es de 9.50m x 4.71m y 2.62 m de alto, área en la que trabajan siete técnicos y en algunos casos también pasantes, además en el mismo lugar se encuentra el cuarto de servidores, esto provoca entre los trabajadores incomodidad al realizar actividades como formateo, mantenimiento, actualizaciones de hardware en los equipos ya que por no contar con el espacio físico adecuado (Figura 3) debe realizarse en el mismo lugar de trabajo del usuario, ocasionando esto, un malestar entre los usuarios y los técnicos.

Figura 3. Desorden y poco espacio físico.

Debido a este problema el cuarto de servidores el cuál tiene las siguientes dimensiones (3.75m x 2.05), no tienen un adecuado orden tanto de los equipos como de los cables de red y cables eléctricos ya que dentro de éste no solo cuentan con servidores sino además con anaqueles, cartones, equipos en mal estado que son retirados por deterioro que tiene algún desperfecto, cabina de central telefónica, bases de Motorolas, entre otros. Ver figuras.

Figura 4. Rack.

Figura 5. Routers.

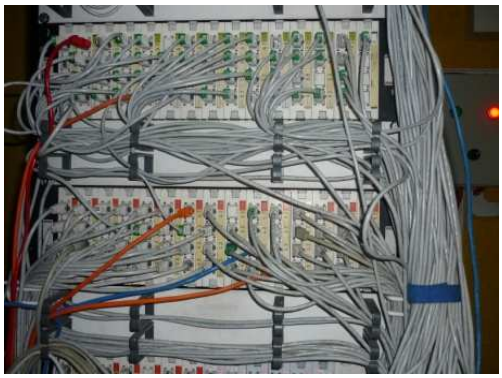


Figura 6. Paneles para Voz y Datos

Figura 7. Equipos Obsoletos y cajas de cartón con periféricos y cables en mal estado.

Figura 8. Panel Eléctrico del Cuarto de Servidores

Figura 9. Base Motorola

En lo referente a la red física el cableado estructurado de red tiene un periodo de ocho años, este es el último cableado que se realizó, no obstante existe otro más antiguo, el cual todavía no se es retirado de las canaletas y sus puntos todavía están visibles.

Figura 10. Cables y canaletas de redes anteriores aun visibles

1.2 PLANEAMIENTO DEL PROBLEMA

La Dirección Provincial de Salud de Pichincha es una Institución Pública que no ha tenido una organización definida en el control de la Seguridad de la red, tanto: en la seguridad física ya que no existe una intervención en la protección del hardware y de los soportes de datos; como en seguridad lógica que no se cuenta con la protección de los datos, procesos y programas, provocando muchos inconvenientes como: pérdidas de información, desconexión de los equipos de computo hacia la red inalámbrica en reiteradas ocasiones por virus, como también el ingreso de diferentes amenazas accidentales: terremotos, inundaciones, influencias Electromagnéticas nocivas, errores de utilización, negligencia del personal, fallo del suministro eléctrico, averías del hardware, fallo del Software, delito contra intimidad; y/o amenazas intencionales: robo, fraude, utilización abusiva del computador, uso no autorizado de la información, etc.

El Departamento de Gestión Informática y Sistemas de la DPSSP esta consiente de todas esta eventualidades y es por eso que se ve en la necesidad de la obtención de un conjunto de procedimientos y técnicas para evaluar y controlar total o parcialmente los Sistemas Informáticos de esta institución, con el fin de proteger sus activos y recursos, verificando así si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática para conseguir la eficacia exigida en el marco de la organización correspondiente y para esto se desarrollará una Auditoria Informática en la Seguridad de la Red.

1.3 OBJETIVOS

a) Objetivo General

Desarrollar una Auditoria Informática de la Seguridad de la Red Física y Lógica y esta tendrá el propósito de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de la Institución.

b) Objetivos Específicos

i) Analizar la situación actual de la Dirección Provincial de Salud de Pichincha, para conocer el estado en el que se encuentran la Red Física y Lógica.
ii) Aplicar los métodos de Auditoria Informática para estimar en qué estado se encuentran la Red Física y Lógica (Cableada e Inalámbrica).
iii) Elaborar un instructivo con procedimientos a seguir para el mejoramiento de la seguridad de la Red Física y Lógica. Este proceso debe enmarcarse en estándares y/o normas relacionadas a las Seguridades.
iv) Ejecutar el instructivo de procedimientos en el Departamento de Gestión de Sistemas e Informática de la DPSP en el Área de Servidores.
v) Generar informes y/o documentación técnica basada en los resultados.

1.4 JUSTIFICACIÓN

El Departamento de Gestión Informática y Sistemas de la Dirección Provincial de Salud de Pichincha está en una etapa de evolución y mejoramiento en sus servicios, es por eso que se ve en la necesidad de encontrar y enfocar estrategias de seguridad para: las instalaciones, tecnología y sistemas de aplicación & datos, porque estas se encuentran vulnerables o están mal procedidas. A continuación se detallan algunas razones por lo cual es necesaria una auditoria informática:

- No se tiene un buen diseño de la red encontrándose mal distribuidos los puntos de la misma, sin preveer el crecimiento de usuarios.
- El servidor de la red se encuentra saturado, tiene poca capacidad de almacenamiento en disco y de memoria, por lo tanto el acceso a la red es lento y además es portador de un sin número de virus, ya por su poca capacidad de almacenamiento y de recurso se dificulta la instalación de antivirus provocando así la propagación de virus y todo tipo de software malicioso a nivel global de la red, sea esta inalámbrica o cableada.
- El antivirus que se tiene en los equipos de los usuarios no es el más indicado, puesto que este antivirus consume mucho recurso del computador.
- Por otro lado, no todos los computadores tienen esta herramienta, porque existe un limitado número de licencias provocando así un desbalance en el proceso de control de los virus.
- El estado actual en que se encuentran los servidores es preocupante, no teniendo ninguno de éstos un antivirus, hallándose la información vulnerable ante cualquier tipo de amenazas de índole informática.
- Los equipos que se encuentran conectados a la red inalámbrica siempre se desconectan de la misma causando molestias a los usuarios al momento de utilizar los recursos informáticos como: impresoras, Internet, Sistemas de uso internos que se encuentran en un ambiente de red.
- No existen políticas de distribución de la Banda Ancha ni censura.
- Los Access Point no se encuentran en lugares apropiados provocando esto la Pérdida de la señal y siendo fácil de extraerlos.

Ante esta problemática, la mejor opción, será ejecutar una auditoria informática que permita obtener evidencia suficiente y adecuada de las debilidades y amenazas a las que se encuentra expuesta la Red de Datos de la Institución, a fin de ejecutar contramedidas en busca de calidad, eficiencia y efectividad del servicio informático tanto para usuarios internos como externos.

1.5 ALCANCE

El presente proyecto se basará en la realización de una Auditoria Informática de la Seguridad de la Red Física y Lógica para el Departamento de Gestión Informática y Sistemas de la Dirección Provincial de Salud de Pichincha (DPSP) en la ciudad de Quito.

Limitándose a:

- Estudio general de los problemas más relevantes que tiene la Institución en el área de seguridad física y lógica de la infraestructura tecnológica de la red de la DPSP.
- Ejecución del instructivo de procedimientos de Seguridad en el Departamento de Gestión de Sistemas e Informática de la DPSP específicamente en el área de Servidores.
- Entrega de informe y material utilizado para el desarrollo de la Auditoria Informática.
- Recomendaciones basadas en la norma ISO 17799(Código de Buenas Prácticas para la Gestión de la Seguridad de la Información) haciendo relación al tema de Seguridad Física y Lógica de la Red.

Nota:

El mencionado estudio, se realizará en el edificio de la Dirección Provincial de Salud de Pichincha, situado en la ciudad de Quito, en las calles García Moreno N-55 y Mejía.

CAPITULO II

En el presente capítulo, se exhibe el análisis y evaluación de los riesgos tecnológicos a los que están expuestos los recursos informáticos en la Dirección Provincial de Salud de Pichincha (D.P.S.P), como también la identificación de amenazas, vulnerabilidades y las posibles medidas de protección.

2 ANÁLISIS Y EVALUACIÓN DE RIESGOS TECNOLÓGICOS EN LA DPSP

2.1 CONCEPTOS GENERALES

2.1.1 SISTEMA DE INFORMACIÓN

"Un Sistema de Información es un conjunto de procedimientos organizados que, cuando se ejecutan, proporcionan información para la toma de decisiones y/o el control de la organización"[3]

Para que puedan operar los Sistemas de Información, se necesita de dos componentes: equipo computacional y recurso humano.

Todo Sistemas de información realiza cuatro actividades básicas: entrada, almacenamiento, procesamiento y salida de información.

2.1.1.1 Entrada de Información:

Es el medio que se utiliza para ingresar la información, pudiendo ser: teclado, ratón, unidades de diskette, códigos de barras, digitalizadores, monitores sensibles al tacto, la voz, entre otros.

2.1.1.2 Almacenamiento de información:

Independientemente del tipo de entrada se haya utilizado, la información es almacenada en estructuras de información denominadas archivos, como medios de almacenamiento se tienen: discos duros, los discos flexibles o diskettes, discos compactos (CD-ROM), DVD, flash memory, discos duros extraíbles.

[3] Henry Lucas, Sistemas de Información Análisis, Diseño, puesta a punto. Paraninfo,1984, Pág. 17

2.1.1.3 Procesamiento de Información:

Después de almacenar la información, se puede realizar cálculos de acuerdo a la secuencia de operaciones, utilizando datos recientes o datos que se encuentran almacenados.

2.1.1.4 Salida de Información:

Finalmente, después de haber realizado una serie de pasos como la entrada de información, almacenamiento de información, procesamiento, se debe tener una salida que muestre el resultado de lo que se ha procesado, obteniendo como medios de salida: monitores, impresoras, diskettes, cintas magnéticas, altavoces, graficadores y plotters, entre otros; algunas veces la salida de información se convierte en entrada a otros sistemas de información.

En la Figura 11, se puede observar que indistintamente al tipo de entrada que tenga la información (sea manual o automática), ésta ingresa a un proceso, para luego ser almacenada; el almacenamiento interactúa con el proceso en caso de que tenga una petición que exija información almacenada; para concluir, presenta los resultados de la información, de similar modo: sea impresa o a través de cualquier medio electrónico.

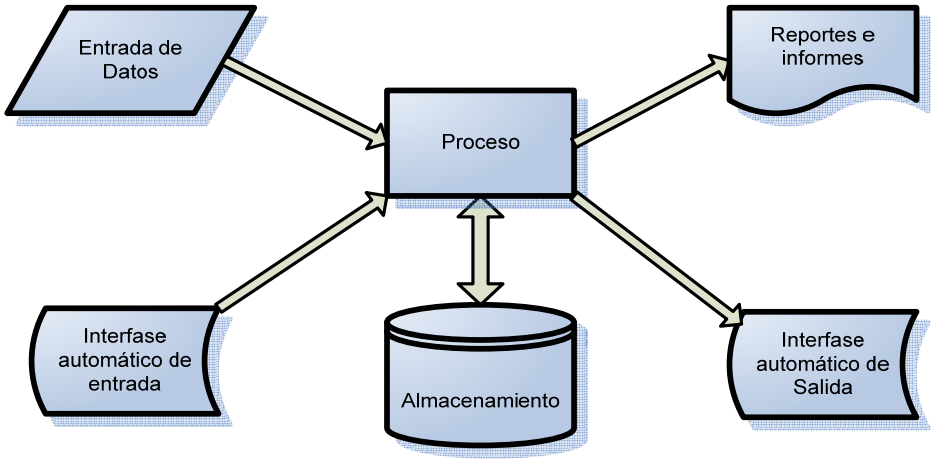


Figura 11. Actividades de los sistemas de información[4]

[4] http://www.monografias.com/trabajos7/sisinf/sisinf.shtml

2.1.2 FUNCIONES DE CONTROL INTERNO INFORMÁTICO

2.1.2.1 Control Interno Informático

El Control Interno Informático controla diariamente que todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijados por la Dirección de la Institución y/o la Coordinación del PGI, así como los requerimientos legales.

El Control Interno Informático suele ser un órgano staff de la Dirección del Departamento de Informática, que tiene como misión asegurarse de que las medidas que se obtienen de los mecanismos implantados por cada responsable sean correctas y válidas; y está dotado de personas y medios materiales según sea la tarea encomendada.

Entre los principales objetivos del Control Interno Informático se pueden indicar los siguientes:

- Controlar que todas las actividades se realizan cumpliendo los procedimientos y normas fijados, y asegurarse del cumplimiento de las normas legales.
- Asesorar sobre el conocimiento de las normas
- Colaborar y apoyar el trabajo de Auditoria informática, así como de las auditorias externas al grupo.
- Definir, implantar y ejecutar mecanismos y controles para comprobar el logro de los grados adecuados del servicio informático, para lo cual cada responsable de objetivos y recursos es responsable de esos niveles, así como de la implantación de los medios de medida adecuados, no es exclusivamente responsabilidad del Control Interno.

Además, el Control Interno Informático debe realizar diferentes actividades operativas dentro de los sistemas (centrales, departamentales, redes locales, PC, etc.) y entornos informáticos (producción, desarrollo o pruebas) como:

- Vigilancia sobre el control de cambios y versiones del software, es decir cumplimiento de procedimientos, normas y controles dictados.
- Controles sobre la producción diaria.

- Controles sobre la calidad y eficiencia del desarrollo y mantenimiento del software y del servicio informático.
- Controles en las redes de comunicaciones.
- Controles sobre el software de base
- Controles en los sistemas microinformáticos.
- Seguridad Informática (su responsabilidad puede estar asignada a control interno o también puede asignársele la responsabilidad de control dual de la misma cuando está encargada a otro órgano):
    - Usuarios, responsables y perfiles de uso de archivos y bases de datos.
    - Normas de seguridad.
    - Control de información clasificada.
    - Control dual de la seguridad informática.
- Licencias y relaciones contractuales con terceros.
- Asesorar y transmitir cultura sobre el riesgo informático.

2.1.2.2 Sistema de Control Interno Informático

Puede definirse como “cualquier actividad o acción realizada manual y/o automáticamente para prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para conseguir sus objetivos”

Los controles internos evolucionan día a día a medida que los sistemas informáticos se vuelven complejos. Para asegurar la integridad, disponibilidad y eficacia de los sistemas informáticos se utilizan mecanismos de control, manuales y en la mayoría de las veces automáticos, aunque en algunos casos dependen de la combinación de elementos de software y de procedimientos.
Por la complejidad de los mecanismos de control es posible asegurar la integridad, disponibilidad y eficacia de los sistemas.

Los objetivos de los controles informáticos se han clasificado en las siguientes categorías:

- Controles preventivos:

Tratan de evitar el hecho, como un software de seguridad que impida los accesos no autorizados al sistema.

- Controles detectivos:

Cuando fallan los preventivos para tratar de conocer cuanto antes el evento. Por ejemplo el registro de intentos de accesos no autorizados.

- Controles correctivos:

Facilitan la vuelta a la normalidad cuando se han producido incidencias. Por ejemplo, la recuperación de un fichero dañado a partir de las copias de seguridad.

2.1.3 AUDITORÍA INFORMÁTICA[5]

Auditoría informática, es el proceso de recoger, agrupar y evaluar evidencias para determinar si un Sistema de Información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas.

También permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos, identificando necesidades, duplicidades, costes y barreras, que obstaculizan flujos de información eficientes.

Auditar consiste principalmente en estudiar los mecanismos de control que están implantados en una empresa u organización, determinando si los mismos son adecuados y cumplen con determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de los mismos. Los mecanismos de control pueden ser directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia.

Los objetivos de la Auditoría Informática son:

- El control de la función informática
- El análisis de la eficiencia de los Sistemas Informáticos
- La verificación del cumplimiento de la Normativa en este ámbito

[5] http://es.wikipedia.org/wiki/Auditor%C3%ADa

- La revisión de la eficacia en la gestión de los recursos informáticos.

La auditoría informática sirve para mejorar ciertas características en la empresa como:

- Eficiencia
- Eficacia
- Rentabilidad
- Seguridad

2.1.3.1 Tipos de Auditoría informática [6]

Dentro de la auditoría informática se destacan los siguientes tipos:

2.1.3.1.1 Auditoría de la gestión:

Referido a la contratación de bienes y servicios, documentación de los programas.

2.1.3.1.2 Auditoría legal del Reglamento de Protección de Datos:

Cumplimiento legal de las medidas de seguridad exigidas por el Reglamento de desarrollo de la Ley Orgánica de Protección de datos.

2.1.3.1.3 Auditoría de los datos:

Clasificación de los datos, estudio de las aplicaciones y análisis de los flujogramas.

2.1.3.1.4 Auditoría de las bases de datos:

Controles de acceso, de actualización, de integridad y calidad de los datos.

2.1.3.1.5 Auditoría de la seguridad:

Referidos a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y no repudio.

[6] Auditoria aplicada a la seguridad en redes de computadores- Monografias_com.mht

2.1.3.1.6 Auditoría de la seguridad física:

Referido a la ubicación de la organización, evitando ubicaciones de riesgo, y en algunos casos no revelando la situación física de esta. También está referida a las protecciones externas (arcos de seguridad, CCTV, vigilantes.) y protecciones del entorno.

2.1.3.1.7 Auditoría de la seguridad lógica:

Comprende los métodos de autenticación de los sistemas de información.

2.1.3.1.8 Auditoría de las comunicaciones.

Se refiere a la auditoria de los procesos de autenticación en los sistemas de comunicación.

2.1.3.2 Objetivos de la Auditoría Informática[7]:

1. Prestar colaboración a la Auditoría de Cuentas:

Se hace difícil en la actualidad llevar un buen control de la actividad económica-financiera de las Instituciones como resultado del alto grado de informatización de las mismas, por medio de la auditoría de cuentas, por lo que necesita de la Auditoría Informática para llevar a cabo su propósito.

2. Auditoría de los propios Sistemas Informáticos:

En este punto, se debe resaltar no sólo el aspecto del control informático en sí, sino también el desarrollo de la seguridad, economía, adecuación de la infraestructura informática de la empresa, entre otros, que hará posible el funcionamiento con eficacia y eficiencia del sistema informático.

3. Prevención de fraude y obtención de la prueba:

De esta manera, se persigue al fraude y se puede obtener la prueba del mismo, trayendo como consecuencia que la información que se aprecie no haya sido manipulada de mala fe antes de hacerse visible y posteriormente.

[7] http://www.monografias.com/trabajos22/auditoria-informatica/auditoria-informatica.shtml

2.1.4 ADMINISTRACIÓN DE LOS RIESGOS INFORMÁTICOS:

La administración de riesgos es una aproximación científica del comportamiento de los riesgos, anticipando posibles pérdidas accidentales con el diseño e implantación de procedimientos que minimicen la ocurrencia de Pérdidas o el impacto financiero de las pérdidas que puedan ocurrir.

2.1.4.1 ¿Qué es Riesgo?

Como la Real Academia de la Lengua manifiesta: “Riesgo es una contingencia o posibilidad de que suceda un daño, desgracia o contratiempo”.

El riesgo también es conocido como la probabilidad de pérdida la cual permite cuantificar el riesgo a diferencia de la posibilidad de riesgo donde este no se puede cuantificar.

El riesgo es incertidumbre relacionado con la duda ante la posible ocurrencia de algo que puede generar pérdidas.

2.1.5 RIESGOS INFORMÁTICOS[8]:

Es importante en toda organización contar con una herramienta, que garantice la correcta evaluación de los riesgos, a los cuales están sometidos los procesos y actividades que participan en el área informática; y por medio de procedimientos de control se pueda evaluar el desempeño del entorno informático.

Una de las principales causas de los problemas dentro del entorno informático, es la inadecuada administración de riesgos informáticos, esta información sirve de apoyo para una adecuada gestión de la administración de riesgos, basándose en los siguientes aspectos:

- La evaluación de los riesgos inherentes a los procesos informáticos.
- La evaluación de las amenazas ó causas de los riesgos.
- Los controles utilizados para minimizar las amenazas a riesgos.
- La asignación de responsables a los procesos informáticos.
- La evaluación de los elementos del análisis de riesgos.

[8] Sistema de Administración de Riesgos en Tecnología Informática, Autor: Alberto Cancelado

Los sistemas de información computarizados son vulnerables a una diversidad de amenazas y atentados por parte de:

- Personas tanto internas como externas de la organización.
- Desastres naturales.
- Servicios, suministros y trabajos no confiables e imperfectos.
- Incompetencia y las deficiencias cotidianas.
- Abuso en el manejo de los sistemas informáticos.
- Desastre a causa de intromisión, robo, fraude, sabotaje o interrupción de las actividades de cómputos.

Todos estos aspectos hacen que sea necesario replantear la seguridad con que cuenta hasta ahora la Institución.

2.1.5.1 Riesgos relacionados con la Informática

En efecto, las principales áreas en que habitualmente ha incursionado la seguridad en las áreas de cómputos han sido:

- Seguridad física.
- Control de accesos.
- Protección de los datos.
- Seguridad en las redes.

2.1.5.2 Riesgos de Integridad:

Este tipo de riesgo afecta directamente a todos los activos informáticos dentro de una organización, como son: la información, los datos, y los sistemas que pueden ser modificados o alterados en su estructura o contenido de manera casual o intencionada por personal no autorizado, poniendo en peligro la integridad de los mismos.

La integridad puede perderse por errores de programación (buena información es procesada por programas mal construidos), procesamiento de errores (Administración pobre del mantenimiento de sistemas)

2.1.5.3 Riesgos de Acceso:

Son ocasionados por el mal manejo de autorización a los sistemas, datos, aplicaciones, programas, información y uso de dispositivos informáticos.

2.1.5.4 Riesgos de Infraestructura:

Son aquellos riesgos de estructura de información tecnológica como hardware, software, redes, personas y procesos; que no se abastecen al crecimiento de la organización y representan costos.

2.1.5.5 Riesgos de seguridad general:

- Riesgos de choque eléctrico: Niveles de alto voltaje.
- Riegos de incendio: Inflamabilidad de materiales.
- Riesgos de niveles inadecuados de energía eléctrica.
- Riesgos de radiaciones: Ondas de ruido, de láser y ultrasónicas.
- Riesgos mecánicos: Inestabilidad de las piezas eléctricas.

2.1.5.6 Riesgos a los cuales se encuentran inmersos los Sistemas de Información

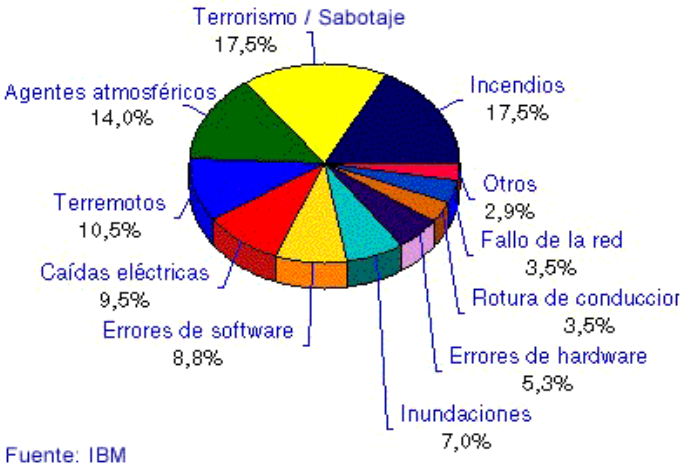


Figura 12. Tipos amenazas de la información

2.1.6 GESTIÓN DE LA SEGURIDAD INFORMÁTICA

La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información ahí contenida, así como su modificación, sólo será accesible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Aunque a simple vista se puede entender que un Riesgo y una Vulnerabilidad se podrían englobar en un mismo concepto, una definición más informal denota la

diferencia entre riesgo y vulnerabilidad, de modo que la Vulnerabilidad está ligada a una Amenaza y el Riesgo a un Impacto.

Es importante tomar en consideración, que las amenazas no disminuirán y las vulnerabilidades no desaparecerán en su totalidad, por lo que los niveles de inversión en el área de seguridad en cualquier empresa, deberán ir acordes a la importancia de la información en riesgo.

2.1.6.1 Objetivos de la Seguridad Informática

Los activos son los elementos que la seguridad informática tiene como objetivo proteger. Son tres elementos que conforman los activos:

- **Información**

  Es el objeto de mayor valor para una organización, el objetivo es el resguardo de la información, independientemente del lugar en donde se encuentre registrada, en algún medio electrónico o físico.

- **Equipos que la soportan**

  Software, hardware y organización.

- **Usuarios**

  Individuos que utilizan la estructura tecnológica y de comunicaciones que manejan la información.

2.1.6.2 Seguridad Lógica [9]

La seguridad lógica se encarga de los controles de acceso que están diseñados para salvaguardar la integridad de la información almacenada de una computadora, así como de controlar el mal uso de la información.

La seguridad lógica se encarga de controlar y salvaguardar la información generada por los sistemas, por el software de desarrollo y por los programas en aplicación, identifica a cada usuario y sus actividades en el sistema, y restringe el acceso a datos, a los programas de uso general, de uso específico, de las redes y terminales.

La falta de seguridad lógica o su violación puede traer las siguientes consecuencias a la organización:

[9] Auditoria Informática, Autor: José Antonio Echenique García

- Cambio de los datos antes o cuando se le da entrada a la computadora.
- Copias de programas y/o información.
- Código oculto en un programa.
- Entrada de virus.

La seguridad lógica puede evitar una afectación de pérdida de registros, y ayuda a conocer el momento en que se produce un cambio o fraude en los sistemas.
Es importante considerar el grado de actuación que puede tener un usuario dentro de un sistema, ya sea que la información se encuentre en un archivo normal o en una base de datos, o bien que se posea una mini computadora, o un sistema en red (interna o externa). Para esto se puede definir los siguientes tipos de usuarios:

- Administrador.
- Usuario principal.
- Usuario de consulta.
- Usuario de explotación.
- Usuario de auditoría.

Para conservar la integridad, confidencialidad y disponibilidad de los sistemas de información se debe tomar en cuenta lo siguiente:

- La integridad es responsabilidad de los individuos autorizados para modificar datos o programas (usuario administrador) o de los usuarios a los que se otorgan accesos a aplicaciones de sistemas o funciones fuera de sus responsabilidades normales de trabajo (usuario responsable y principal).
- La confidencialidad es responsabilidad de los individuos autorizados para consultar (usuario de consulta) o para bajar archivos importantes para microcomputadoras (usuario de explotación).
- La disponibilidad es responsabilidad de individuos autorizados para alterar los parámetros de control de acceso al sistema operativo, al sistema manejador de base de datos, al monitoreo de teleproceso o al software de telecomunicaciones (usuario administrador).

La seguridad lógica abarca las siguientes áreas:

- Rutas de acceso (pasar por uno o múltiples niveles de seguridad antes de obtener el acceso a los programas y datos).
- Claves de acceso (identificar a un usuario de otros).
- Software de control de acceso (graba los eventos realizados y el acceso a los recursos identificando al usuario que lo realiza).

  En telecomunicaciones este tipo de software provee la interfaz entre las terminales y las redes, permitiendo realizar las siguientes acciones:
  - Controlar la invocación de los programas de aplicación.
  - Verificar que todas las transacciones estén completas y sean correctamente transmitidas.
  - Restringir a los usuarios para actuar en funciones seleccionadas.
  - Restringir el acceso al sistema a ciertos individuos
- Encriptamiento (transformación de los datos a una forma que no sea posible leerla por cualquier persona).

2.1.6.3 Seguridad Física Vs. Seguridad Lógica[10]

Todas las amenazas a las que está sometido un Sistema de Información, así como las medidas de protección y salvaguarda que se implantan en dicho sistema para garantizar la Seguridad de la Información, tienen que ver con las amenazas de carácter lógico o físico, y de las medidas de Seguridad Lógica y Seguridad Física.

Las amenazas de tipo lógico suelen comprometer tanto la Confidencialidad, como la Integridad y Disponibilidad de la información, sin embargo, las amenazas físicas atacan en mayor medida a la Disponibilidad, aunque también existen amenazas de carácter físico sobre la Confidencialidad e Integridad para las que son necesarias implementar medidas de protección y salvaguarda de carácter físico.

La Seguridad Lógica es la rama de la Seguridad informática más conocida y se le otorga mayor importancia, pero hay que tener en cuenta que los incidentes de seguridad que ponen en peligro la continuidad del servicio e incluso hasta la existencia de la organización, están comprendidos dentro del ámbito de la Seguridad física.

[10] Auditoría de Tecnologías y Sistemas de Información, Autor: Ricardo Cañizares Sales

Un ataque lógico a un Sistema de Información puede comprometer su funcionamiento y dejarlo fuera de servicio durante un período de tiempo más o menos largo, un ataque físico puede dejarlo inoperativo para siempre.
Se ha comprobado que la amenaza más grave a la que está sujeto el hardware es un ataque malintencionado, debido a que existe voluntad de hacer daño y se suele dirigir contra el elemento más débil, habitualmente con menos protección y que más impacto causa en la organización cuando es destruido.

2.2 IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES DE ÍNDOLES TECNOLÓGICAS, AMBIENTALES, Y HUMANAS.

Como se observó que el Proceso de Gestión Informática tiene organizadas sus actividades por áreas y de acuerdo a eso se realizará el análisis de las diferentes amenazas y vulnerabilidades existentes en dicho proceso.

2.2.1 IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES-TECNOLÓGICAS

En las siguientes tablas se visualiza las amenazas y vulnerabilidades tecnológicas a los que están expuestos los recursos informáticos en la DPSP, desde sus diferentes áreas.

- **Área de Hardware y Software:**

AMENAZAS	VULNERABILIDADES
Sabotaje interno, mal uso de los recursos informáticos de la institución	Falta de control de acceso a los Sistemas y Base de Datos.
Ataques de Códigos Maliciosos (Hackers, Bombas Lógicas, Troyanos, etc.)	Equipos desprotegidos de herramientas de antivirus y Spam
Daños severos e inestabilidad en los Sistemas y/o Bases de Datos.	Inexistencias de Registro de Anomalías de los diferentes Software (Síntomas de problemas y mensajes de error o distintas advertencias).

Tabla 10. Listado de Amenazas y Vulnerabilidades Tecnológicas-Hardware & Software

- **Área de Comunicaciones:**

AMENAZAS	VULNERABILIDADES
Virus, Spams, Hackers, etc.	Inexistencia de Firewall Físico y Lógico.
Desactivación errada a equipos	No existe rotulación en los equipos de comunicación (Routers, Switch, Access Point, etc.)

Tabla 11. Listado de Amenazas y Vulnerabilidades Tecnológicas-Comunicaciones

2.2.2 IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES-AMBIENTALES

En las siguientes tablas se mencionan las amenazas y vulnerabilidades ambientales a los que están expuestos los recursos informáticos en la DPSP, desde sus diferentes áreas.

- **Áreas de Hardware y Software:**

AMENAZAS	VULNERABILIDADES
El Área de Computo se sobrecalienta o se congela el ducto del aire acondicionado, provocando goteo al momento de descongelar.	Deficiencia en las Unidades de Aire Acondicionado.
En caso de inundación por la avería de tuberías, los equipos se dañarían y se compromete el procesamiento de la información	Los equipos de computo y servidores, UPS, reguladores, etc. Se encuentran situados en el piso.
El Smoke afecta a las partes y piezas de los equipos de computación principalmente a los monitores e impresoras.	Por encontrarse en un lugar céntrico, de excesivo congestionamiento vehicular, la Institución se encuentra expuesta a la contaminación ambiental.

Tabla 12. Listado de Amenazas y Vulnerabilidades Ambientales-Hardware & software

- **Área de Comunicaciones:**

AMENAZAS	VULNERABILIDADES
Inexistencias de Filtros contra Rayos en las Líneas de Comunicación Externa.	Pérdida del enlace constantes en las áreas de salud.

Tabla 13. Listado de Amenazas y Vulnerabilidades Ambientales-Comunicaciones

2.2.3 IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES-HUMANAS

En las siguientes tablas se señala las amenazas y vulnerabilidades humanas a los que están expuestos los recursos informáticos en la DPSP, desde sus diferentes áreas.

- **Área Hardware**

AMENAZAS	VULNERABILIDADES
Pérdidas de equipos	No existe control de salida de equipos
Inestabilidad Sistema Eléctrico	No se realiza un mantenimiento preventivo del Sistema Eléctrico
Agitación civil	Por la ubicación física de la DPSP (cerca del Palacio de Carondelet) se está siempre expuesto a turbas o protestas.
Pérdida del servicio de red dentro de la Institución	No disponen de instrumentos para mantenimiento de la red.
Duplicidad en gastos, por desconocer si el equipo dañado tiene o no garantía.	Inexistencia de Registro de Garantía
Desconocimiento de especificaciones técnicas y el número exacto de los computadores con los que cuenta la Institución.	Inexistencias Parque Informático
Que se quemen los equipos computacionales	Pérdidas constantes de energía.

Que por similitud se de formato al servidor incorrecto	No existe etiquetación de los Servidores.
Desperfecto de los equipos ocasionado Pérdida del servicio de Internet y/o enlace de datos desde la DPSP hacia las diferentes áreas de Salud.	No existe mantenimiento preventivo ni correctivo de los equipos de comunicación(router, switch,)
Pérdida de productividad por parte del personal que no cuenta con sus equipos	Equipos que se quedan sin reparación por falta de presupuesto.

Tabla 14. Listado de Amenazas y Vulnerabilidades Humanas-Hardware

- **Área de Software:**

AMENAZAS	VULNERABILIDADES
Desconocer que Aplicaciones, Sistemas y/o bases de datos han sido actualizados.	Falta de control de registro de versiones
Sabotaje interno, mal uso de los recursos informáticos de la institución	Falta de control de acceso a los Sistemas y Base de Datos.
Pérdida de la información por falta de control de respaldos.	Inexistencias de etiquetación, control y registro de los backups.
No brindar un buen soporte y administración en los diferentes aplicaciones y/o bases de datos.	No existen Manuales Técnicos de los Diferentes Sistemas.
Computadores no cuentan con protección de Antivirus	Escaso número de licencia de antivirus
Daño de equipo o software por los usuarios	Usuarios con bajo Nivel Informático
Contaminación y Propagación de virus	Utilización inapropiada del Internet
Manipulación de las Bases de Datos por usuarios internos.	No existen Manuales Técnicos de los Diferentes Sistemas.
Incumpliendo con una norma – Ley(Decreto 1014 para el uso de Software	Inexistencias de Licencias del Sistema Operativo para la Mayoría de

Libre en Ecuador)	computadores

Tabla 15. Listado de Amenazas y Vulnerabilidades Humanas-Software

- **Área de Comunicaciones:**

AMENAZAS	VULNERABILIDADES
Pérdida de Productividad	Constantes caídas de los enlaces
Pérdidas Inesperadas de la señal	No existe un Monitoreo de los Enlaces
Los técnicos no identifican a los equipos, provocando errores.	No existe rotulación en los equipos de comunicación (routers, switch, Access point y hubs.)
Pérdida de Paquetes inexplicables	No existe un Monitoreo de los Enlaces
Saturación de la Red – Usuario sin puntos de red asignados	No existe una Planificación de Cableado
Pérdida de Productividad e Información	No existe Planificación de la recuperación de las comunicaciones en caso de desastre.
Ineficiente Procedimiento de administración de la red	No existe documentación actualizada del diagramado de la red.
Ineficiente Procedimiento de administración de la red	No existe registro actualizado de módems, controladores, terminales, líneas y todo equipo relacionado con las comunicaciones.
Duplicidad de IP en computadores y/o equipos informáticos	No existe un registro de asignación de IP para los equipos.
Access Point en lugares poco seguros	Inexistencias de Estudio Técnico de Factibilidad para la red inalámbrica

Tabla 16. Listado de Amenazas y Vulnerabilidades Humanas-Comunicaciones

2.3 ANÁLISIS - EVALUACIÓN DE RIESGOS DE LA GESTIÓN DE SEGURIDAD DE LA DPSP[11]

El análisis de riesgo (también conocido como evaluación de riesgo), identifica las amenazas, vulnerabilidades y riesgos de la información, sobre la plataforma tecnológica de una organización, con el fin de generar un plan de implementación de los controles que aseguren un ambiente informático seguro, bajo los criterios de disponibilidad, confidencialidad e integridad de la información.

Los dos puntos importantes a considerar son:

- La probabilidad de una amenaza
- La magnitud del impacto sobre el sistema, la cual se mide por el nivel de degradación de uno o combinación de alguno de los siguientes elementos: confidencialidad, disponibilidad, integridad.

Al conocer de la existencia de riesgos se debe pensar en qué hacer con ellos una vez identificados, pudiéndose:

- **Mitigar el riesgo,** mediante la implantación y mantenimiento de controles de seguridad que minimicen estos riesgos y los mantengan a un nivel aceptable (lo cual implica inversiones económicas)
- **Asumir el riesgo** ciertos riesgos a los que está expuesta la organización ya que las consecuencias acarrean un coste económico y estratégico menor que el coste que sería necesario aportar para reducir dichos riesgos
- **Transferir el riesgo** estos riesgos, bien a un prestador de servicios especializado mediante la contratación de una póliza de riesgo electrónico.

A pesar de ser un procedimiento que se puede ejecutar de forma sistemática, en un análisis de riesgos es necesario realizar determinadas tareas, en este caso se utiliza las NIST (Instituto Nacional de Estándares y Tecnología) Special Publication 800-30:

- Paso 1. Sistema de caracterización.

[11] http://74.125.93.132/search?q=cache:-uGezw_rQFAJ:www.fistconference.org/data/presentaciones/AnalisisyGestiondeRiesgos.pdf+evaluacion+de+riegos%2Banalisis+de+riesgos+informaticos&cd=4&hl=es&ct=clnk&gl=ec

- Paso 2. Identificación de Amenazas.
- Paso 3. Identificación de Vulnerabilidades.
- Paso 4. Análisis del control.
- Paso 5. Determinación de Riesgo.
- Paso 6. Análisis del impacto.
- Paso 7. Determinación de probabilidades.
- Paso 8. Recomendaciones de los controles.

Si estos factores no se evalúan con total imparcialidad y objetividad, el análisis de riesgos no podrá cumplir su función con garantías, que es ayudar a tomar decisiones sobre cómo proteger los activos de la organización.

2.3.1 PASO 1: SISTEMA DE CARACTERIZACIÓN

Es identificar donde se va a realizar la evaluación del riesgos, los límites del Sistema de TI, los recursos y la información que constituye el Sistema.

2.3.1.1 Paso 1.1: Sistema de Información de TI.

Describe todo lo que es parte de los Sistemas de Información como por ejemplo: hardware, software, recursos de comunicaciones, datos e información crítica, personas que apoyan y utilizan el sistema de TI.

A continuación se detalla cada uno de los puntos mencionados mediante tablas:

- **Recursos Hardware**[12]

En la siguiente tabla se describe las características principales de los servidores que mantiene el Proceso de Gestión Informática de la DPSP.

MARCA	MODELO	CARACTERÍSTICAS TÉCNICAS	SISTEMA OPERATIVO	IP	ASIGNACIÓN
HP	PROLIANT ML-370G5	PROCESADOR: INTEL XEON 2.66G. RAM: 16.0 G	WINDOWS 2003 SERVER	10.64.33.250 10.64.32.39	Servidor de Aplicaciones alberga 2 máquinas virtuales 1.- Servidor de Dominio PICDPSP(usuarios e impresoras de este dominio) 2.- Sistemas: VGSIPF, Control de Correspondencia, Transportes , Lexis, GSM
HP	ML-150	PROCESADOR: INTEL XEON 3.0 G RAM: 512	LINUX CENTOS 4.0	10.64.32.51	Servidor de Internet, Correo Electrónico, Alberga la página Web

[12] ANEXO 1. Resumen de inventario de hardware de algunos Servidores y Equipos de usuarios

HP	2120	PROCESADOR: INTEL XEON 2.8 G RAM: 1G	WINDOWS 2003 SERVER	10.694.32.41	Servidor Citrix
HP	PROLIANT ML-370	PROCESADOR: INTEL XEON 3.6 G RAM: 5.93G	WINDOWS 2003 SERVER	10.64.32.18	Servidor de Dominio
CLON	PENTIUM IV	PROCESADOR: INTEL PENTIUM IV 1.2 G RAM: 1G	WINDOWS 2003 SERVER	10.64.34.1	Servidor Sistema Gestor
CLON	PENTIUM IV	PROCESADOR: INTEL PENTIUM IV 1.2 G RAM: 1G	WINDOWS 2003 SERVER	10.64.32.38	Servidor Antivirus Panda
CLON	PENTIUM IV	PROCESADOR: INTEL PENTIUM IV 1.2 G RAM: 1G	WINDOWS 2003 SERVER	10.64.32.22	Servidor Sistema SISPROD

Tabla 17. Listado de los Servidores con su asignación - Hardware

- **Recursos Software**

  En la siguiente tabla se describe los diferentes sistemas implementados e instalados en los servidores que mantiene el Proceso de Gestión Informática de la DPSP.

NOMBRE	PARA EL PROCESO DE:	DESARROLLADO EN:	BASE DE DATOS
GESTOR (ERP)	FARMACIA	ORACLE6I	ORCALE 9I
VGSIPF	CONTROL Y VIGILANCIA SANITARIA	VISUAL BASIC	SQL SERVER
SISPROD	ESTADISTICA	VISUAL FOXPRO	MYSQL
SGM	AREAS DE SALUD(5, 6 Y 8)	VISUAL BASIC	MYSQL
ANGEL	AREAS DE SALUD (9,2,13 Y 8)	JAVA	MYSQL
SIGEF	FINANCIERO	POWER BUILDER	ORACLE
CONTROL DE CORRESPONDENCIA	SECRETARIA GENERAL	. NET	MYSQL
TRANSPORTES	CONTROL Y VIGILANCIA SANITARIA	. NET	MYSQL

Tabla 18. Listado de los Sistemas Informáticos implementados - Software

- **Herramientas Informáticas:**

En la siguiente tabla se describe las diferentes herramientas informáticas que se mantiene en la DPSP.

NOMBRE	PARA EL PROCESO DE:	DESCRIPCIÓN
LEXIS	JURÍDICO	HERRAMIENTA DE BÚSQUEDA DE DOCUMENTOS LEGALES Y REGISTROS OFICIALES
NET SOPPORT	INFORMÁTICA (HACIA TODOS LOS USUARIOS)	HERRAMIENTA PARA SOPORTE REMOTO
CITRIX	FARMACIA SUR	HERRAMIENTA DE CONEXIÓN REMOTA
PANDA	EL 50% DE LOS USUARIOS	CONSOLAS DE ANTIVIRUS

Tabla 19. Listado de Herramientas Informáticas - Software

- **Sistemas Operativos**

En la siguiente tabla se describe los diferentes Sistemas Operativos que se utilizan en la DPSP.

NOMBRE		INSTALADO EN:
Windows 2000	SERVICE PACK 4	DESKTOP- Usuarios
Windows XP	SERVICE PACK 2	DESKTOP- Usuarios
Windows Vista	-	DESKTOP- Usuarios
Windows 2000 Server	SERVICE PACK 2	SERVIDORES
Windows 2003 Server	-	SERVIDORES
Linux CentOS 10.0	-	SERVIDOR

Tabla 20. Listados de los Sistemas Operativos - Software

- **Recursos Comunicaciones**

En la siguiente tabla se detallan las características principales de los equipo de comunicación que mantiene la DPSP

EQUIPO	MARCA	MODELO
ROUTER	CISCO	1700
ROUTER	CISCO	1700
ROUTER	CISCO	1600
ACCESS POINT	LINKSYS	WIRELESS-G
HUB	ACERHUB	116/16 PUERTOS
HUB	CISCO	24 PUERTOS
HUB	CISCO	24 PUERTOS
SWITCH	LINKS	48 PUERTOS
SWITCH	LINKS	48 PUERTOS
SWITCH	DLINK	DES-3226L
SWITCH	ETHERNET SWITCH	24 PUERTOS

Tabla 21. Listado de Equipos de Comunicaciones

- **Datos e Información Critica**

En la siguiente tabla se detallan el recurso crítico para el PGI.

RECURSO	DESCRIPCIÓN
Base de Datos VGSIPF	Base de Datos del Sistema de Control Sanitario
Base de Datos Gestor	Base de Datos del Sistema de Farmacia
Base de Datos SGM	Base de Datos del Sistema de Historias Clínicas
Base de Datos SISPROD	Base de Datos del Sistema de Estadísticas de Salubridad a nivel Provincial y Nacional

Información manejada por Usuarios	Ciertos Usuarios maneja información sensible y muy importante para cada uno de los departamentos e Institución

Tabla 22. Listado de Datos e Información Crítica

- **Usuarios del Sistema.**

  La creación de los usuarios se realiza a petición verbal del mismo usuario, conjuntamente con el equipo que se le asignará, cuyos perfiles son de Usuarios Restringidos.

- **Personas que apoyan los Sistemas de TI**
  - Ing. Maritza Badillo Coordinadora del Proceso
  - Egr. Sonia Buñay
  - Egr. Xavier Morales
  - Sr. Guillermo Mantilla
  - Sr. Wilson Carvajal
  - Egr. Patricia Jácome
  - Sr. Henry Rosero
  - Lcda. Mariana Vergara (Secretaria)
- **Políticas de Seguridad de TI.**

  Políticas de Seguridad actualmente no existen, la DPSP solo cuenta con Políticas para el uso de los computadores[13], las mismas que han sido entregadas a todos los usuarios en el año 2007. Este documento no ha sido, actualizado, ni tampoco dado a conocer a los nuevos usuarios.

- **Protección de almacenamiento de información**

  No se tiene ningún tipo de protección que salvaguarde la información para mantener su disponibilidad, integridad y confidencialidad de los datos.

- **Controles utilizados para el Sistema de TI**

  No existen normas de comportamiento de seguridad y planificación para los Sistemas de TI.

- **Entorno de Seguridad Física:**

  La única seguridad física que existe es al ingresar o salir del edificio, contando con un agente de seguridad proporcionado por una compañía de guardianía privada, excepto el PGI, el cual cuenta con un dispositivo

[13] Anexo 3. Políticas para el uso de los Computadores de la DPSP

detector de tarjetas magnéticas para el cual solo tienen acceso el personal del PGI, pero esta seguridad es irreal ya que la puerta permanece abierta.

- **Seguridad Ambiental de Sistemas TI**

  El cuarto de Servidores se encuentra dentro del área del Proceso de Gestión Informática, además cuenta con dos Equipos de Aire Acondicionado, siete servidores, dos UPS, y ningún extintor tan solo en el PGI, pero este no es el apropiado para este tipo de equipos.

2.3.1.2 Paso 1.2: Técnicas de recolección de la información

Como técnicas de recolección para el análisis de riegos se utilizó lo siguiente:

- Cuestionarios[14]
- Entrevistas: Al realizar estas preguntas se determinó en primera instancia los riegos a los que están expuestos los recursos.

1. **¿Qué puede ir mal en la DPSP?**

   - Que la información se pierda
   - Que los equipos se pierdan (Hurto) o daño
   - Pérdida de Productividad
   - Sabotajes Intencionales
   - Que hackeen los servidores
   - Que los enlaces se caigan

2. **¿Con qué frecuencia pueden ocurrir esos eventos?**

   - Pueden llegar a ocurrir de forma continua

3. **¿Cuáles serían sus consecuencias?**

   - No poder recuperar la información
   - Mucho tiempo en recuperar la información (en el caso que se pueda recuperar)
   - Despido de empleados

[14] ANEXO 4. Evaluación de Seguridades

- Pérdida de la Productividad a Nivel Provincial (en el caso del Sistema de Control Sanitario)
- Inestabilidad de la Institución.

4. **¿Qué fiabilidad tienen las respuestas a las tres primeras preguntas?**

- Alto grado de fiabilidad

5. **¿Se está preparado para abrir las puertas del negocio sin los sistemas, por un día, una semana, cuanto tiempo?**

Para el tipo de servicio y negocio, la Institución no esta preparada para trabajar sin sus sistemas.

6. **¿Cuál es el costo de una hora sin procesar, un día, una semana...?**

Por citar algunos:

Sistema GESTOR: $ 1.000 por cada hora

Sistema VGSIPF: $ 2.000 por cada hora

Sistema SGM, SISPROD, ANGEL, CONTROL DE CORRESPONDENCIA, TRANSPORTES: En estos casos no se generaría Pérdida monetaria, pero tendría un gran quebranto en la calidad de sus servicios.

7. **¿Se tiene forma de detectar a un empleado deshonesto en el sistema?**

A un usuario deshonesto no, pero si se podría detectar el mal uso de los procesos ya sea estos por error o intencional, ya que los sistemas cuentan con registro de auditoria en sus bases de datos.

8. **¿Se tiene control sobre las operaciones de los distintos Sistemas?**

   El Proceso de Gestión Informática no cuenta con ese control, ya que solo se limita a la obtención de respaldos.

9. **¿Qué sistemas necesitan un buen manejo de confidencial y/o sensitiva?**

   Todos los sistemas que utiliza la institución

10. **¿La seguridad actual cubre los tipos de ataques existentes y está preparada para adecuarse a los avances tecnológicos esperados?**

    No, porque no existe ninguna seguridad en ninguna de sus diferentes áreas.

11. **¿Quién es el propietario del recurso? y ¿quién es el usuario con mayores privilegios sobre ese recurso?**

    El propietario de recurso tanto hardware como software es la Institución, los usuarios con mayores privilegios son los técnicos del PGI.

12. **¿Cómo se actuará si la seguridad es violada?**

    Se actuaría tomando acciones de acuerdo al caso.

- **Revisión de Manuales de Procedimientos del Proceso de Gestión Informática.**

  Desafortunadamente el PGI no cuenta con ningún tipo de Manual (manual de usuario[15], manual técnico[16], manual de procedimiento[17]) que pueda ayudar a los técnicos o que pueda ser de conocimiento para ellos mismos de cómo esta cada recurso de TI.

[15] Manual de Usuario.- Guías practicas para el uso de determinados sistemas y/o equipos.
[16] Manual Técnico.- Guías técnicas para el uso de determinados sistemas, equipos, bases de datos, diccionarios de datos.
[17] Manual de Procedimiento.- Establece la forma que se debe operar diferentes procesos.

- **Observación de Sitio.**

  La observación se ha realizado en cada uno de los pisos, recolectando información como: manejo de equipos, entorno, infraestructura de red, etc.

2.3.2 PASO 2 Y PASO 3: IDENTIFICACIÓN DE LAS AMENAZAS-IDENTIFICACIÓN DE LAS VULNERABILIDADES.

Los pasos 2 y 3, se encuentran completados en el Subcapítulo 2.2. Identificación de amenazas y vulnerabilidades de índoles tecnológicas, ambientales, y humanas.

2.3.3 PASO 4: ANÁLISIS DEL CONTROL[18]

- Área de Seguridad Física

  Control encontrado:

  - Servicios de Empresa de Seguridad de Guardianía.
  - Uso de tarjetas magnéticas para ingresar al PGI, solo personal del Proceso.
- Área de Seguridad Lógica

  Control encontrado:

  - Ninguno
- Área de Comunicaciones (Red)

  Control encontrado:

  - Ninguno

2.3.4 PASO 5: DETERMINACIÓN DE PROBABILIDADES[19]

Probabilidad Alto.

Determinación de acuerdo a la vulnerabilidad:

1. Puede resultar la pérdida costosa de los principales activos materiales o recursos;
2. De manera significativa puede violar, dañar, o impedir la misión de una organización, la reputación o intereses, ó

[18] ANEXO 5. Evaluación de Control Interno
[19] Auditoria-NIST-Guía para Gestión de riesgos para sistemas de tecnología de la información

3. Pueden producir la muerte de humanos o lesiones graves.

Probabilidad Medio.

Determinación de acuerdo a la vulnerabilidad:

1. Puede resultar la pérdida de materiales costosos de activos o recursos.
2. Puede violar, dañar, o impedir la misión, la reputación, o interés de la organización,
3. Puede resultar en lesiones personales.

Probabilidad Bajo.

Determinación de acuerdo a la vulnerabilidad:

1. Resultar la pérdida de algunos materiales activos o recursos.
2. Puede afectar notablemente a una organización, la misión, la reputación o intereses. Ver Tabla 23:

TIPO DE RIESGO	FACTOR	PROBABILIDAD
Robo de información	Alto	Bajo - 2
Fallas en los equipos	Alto	Medio – 1
Pérdida de Información	Alto	Alto - 2
Virus Informáticos	Alto	Alto - 1
Accesos no autorizados	Alto	Alto - 2
Fraude Internos o Externos	Alto	Alto - 2
Inestabilidad Sistema Eléctrico	Alto	Alto - 1
Pérdida del enlace de datos	Medio	Bajo - 2
Robo de Servidores	Medio	Bajo - 1
Robo de computadores	Medio	Bajo - 1

Robo de Equipos de Comunicación(Switch, Hubs, Router, Access Point, Antenas de enlace de datos y de tarjetas inalámbricas)	Medio	Medio - 1
Robo de equipos de computo (impresoras, scanner, discos extraíbles, flash memory)	Medio	Bajo - 1
Inundación	Bajo	Medio - 1

Tabla 23. Tipo de Riesgos y su Factor

Como se puede apreciar, en la Tabla 23. Los riesgos se clasifican por su nivel de Impacto o Factor, esta clasificación se basa de acuerdo a la importancia que estos riesgos representan para la Institución y la severidad de su pérdida si ese fuera el caso.

Para la cuantificación del riesgo de perder un recurso, es posible asignar un valor numérico de 0 a 10, tanto a la importancia del recurso (10 es el recurso de mayor importancia) como al riesgo de perderlo (10 es el riesgo más alto).

Para esta cuantificación se determina lo siguiente:

- Estimación del Riesgo de pérdida del recurso (Ri)
- Estimación de la Importancia del recurso (Ii)

El riesgo de un recurso será el producto del riesgo de perderlo por la importancia del recurso.

$$WRi = Ri * Ii \quad \textbf{Ec. 1}$$

Para realizar la evaluación de los diferentes tipos de riesgos citados en la tabla anterior, se realizar su cuantificación respectiva.

A continuación se efectúa la Cuantificación de los Riegos para los recursos más importantes a proteger dentro de la Dirección Provincial de Salud de Pichincha (DPSP).

En la siguiente tabla detallamos los valores que se asignará en la cuantificación de los riesgos de acuerdo a su factor.

FACTOR	RIESGO DE PÉRDIDA DEL RECURSO – Ri	IMPORTANCIA DE RECURSO - Ii
Alta	10	10
Media	5	5
Baja	0	0

Tabla 24. Cuantificación de Riesgos

HARDWARE:

$$WRi = Ri * Ii$$

- **Servidores:**

Hurto: WRi = 0 * 10

WRi = 0

Por lo tanto: » Su riesgo de pérdida es Baja.

Daño Físico: WRi = 10 * 10

WRi = 100

Por lo tanto: » Su riesgo de pérdida es Alta

- **Equipos de Computo:**

Hurto: WRi = 5 * 5

WRi = 25

Por lo tanto: » Su riesgo de pérdida es Media Baja

Daño Físico: WRi = 10 * 5

WRi = 50

Por lo tanto: » Su riesgo de pérdida es Media

- **Routers, Switch, Hubs:**

Hurto: WRi = 0 * 5

WRi = 0

Por lo tanto: » Su riesgo de pérdida es Baja

Daño Físico: WRi = 0 * 5

WRi = 0

Por lo tanto: » Su riesgo de pérdida es Baja

SOFTWARE:

- **Información:(Sistemas y Aplicaciones)**

Hurto/Sabotaje Interno/Pérdida:

WRi = 5 * 10

WRi = 50

Por lo tanto: » Su riesgo de pérdida es Media

Virus/Código malicioso/Sabotaje Electrónico

WRi = 10 * 10

WRi = 100

Por lo tanto: » Su riesgo de pérdida es Alta

COMUNICACIÓN:

- **Enlace de Datos:**

Pérdida de la Señal: WRi = 10 * 10

WRi = 100

Por lo tanto: » Su riesgo de pérdida es Alta

- **Red Inalámbrica:**

Pérdida de la Señal: WRi = 10 * 10

WRi = 100

Por lo tanto: » Su riesgo de pérdida es Alta

- **Red LAN:**

Colapso: WRi = 5 * 10

WRi = 50

Por lo tanto: » Su riesgo de pérdida es Media

Desconexión de Cables de Red: WRi = 10 * 5

WRi = 50

Por lo tanto: » Su riesgo de pérdida es Media

2.3.5 PASO 6, PASO 7 y PASO 8: ANÁLISIS DEL IMPACTO (MATRIZ DE RIESGOS)

En las siguientes tablas, se realiza el análisis de impacto, determinación de probabilidades y generación de recomendaciones para mitigar los riesgos.

- **HARDWARE**

RECURSO	AMENAZA	VULNERABILIDAD	CONTROL EXISTENTE	IMPACTO	PROBABILIDAD	NIVEL DE RIESGO	RECOMENDACIÓN
Servidores	**Mal uso**	No existe políticas de uso para este tipo de equipos	No existe	Alto	Alto	Medio	Establecer un manual de políticas para uso y tratamiento para este tipo de equipo
Computadores	**Mal uso**	El manual de políticas de uso para los computadores no es entregado a todos los usuarios	No existe	Bajo	Bajo	Medio	Entregar el manual de políticas de uso para los computadores a todos los usuarios y solicitar que los usuarios realicen

							revisiones periódicas a este manual.
Laptops, impresoras, discos duros, discos extraíbles	**Hurto**	No existe control al usuario extremo como a los usuarios al momento de salir del edificio	No existe	Bajo	Medio	Bajo	Implementar un sistema de video vigilancia y empresa de seguridad rígida en normas de seguridad.
Equipos de computación	**Que se quemen**	Inestabilidad del sistema eléctrico	No existe	Alto	Alto	Alto	Analizar el sistema eléctrico y tomar correctivos-urgentes.

Tabla 25. Matriz de Riesgos - Hardware

- **SOFTWARE**

RECURSO	AMENAZA	VULNERABILIDAD	CONTROL EXISTENTE	IMPACTO	PROBABILIDAD	NIVEL DE RIESGO	RECOMENDACIÓN
Sistemas	**Mal Uso**	Poca Capacitación a los usuarios	No existe	Alto	Alto	Alto	Reforzamiento de Capacitación, Buen Manejo de Perfil de usuarios en cada sistema
Información	**Pérdida**	No existe un proceso para el tratamiento de los respaldos	No existe	Alto	Alto	Alto	Establecer Políticas de manejo de respaldos tanto para usuarios básicos como técnicos.

Información	**Sabotaje**	No existe un buen manejo de la contraseña del Administrador de los Sistemas.	No existe	Alto	Medio	Alto	Establecer Políticas para el manejo de contraseñas
Bases de Datos	**Mal manejo**	Poca instrucción de los usuarios técnicos en administración de Base de Datos	No existe	Alto	Alto	Alto	Capacitación en administración para las Diferentes Base de Datos que la institución mantiene.

Tabla 26. Matriz de Riesgos - Software

- **COMUNICACIONES:**

RECURSO	AMENAZA	VULNERABILIDAD	CONTROL EXISTENTE	IMPACTO	PROBABILIDAD	NIVEL DE RIESGO	RECOMENDACIÓN
Access Point	**Hurto**	Access Point colocados sobre los escritorios de los usuarios	No existe	Medio	Alto	Alto	Colocar los Access Point en lugares seguros y de mejor propagación de la señal
Router	**Mal Funcionamiento**	No existe etiquetación en estos dispositivos	No existe	Alto	Bajo	Alto	Etiquetar los dispositivos para la correcta identificación de los mismos
Switch	**Mal Funcionamiento**	No existe etiquetación en estos dispositivos	No existe	Alto	Bajo	Alto	Etiquetar los dispositivos para la correcta identificación de los mismos

Access Point	**Mal Funcionamiento**	Poca instrucción de los usuarios técnicos en la configuración de este tipo de dispositivos	No existe	Bajo	Alto	Alto	Capacitación en manejo y configuración de estos dispositivos.

Tabla 27. Matriz de Riesgos - Comunicaciones

2.4 PRESENTACIÓN DE LAS MEDIDAS DE PROTECCIÓN.

Desde el punto de vista técnico, es un poco difícil cuantificar los costos de la información, ya sea para salvaguardarla ó el costo de perderla; porque no se sabe qué valor proporcionarle. Pero a los recursos se debe dar un costo justificable.

2.4.1 EVALUACIÓN DE COSTOS

La evaluación de costos consiste en cuantificar los daños que cada posible vulnerabilidad, pueda causar, teniendo en cuenta las posibilidades de que sucedan, para esto se debe analizar lo siguiente:

- **¿Qué recursos se quieren proteger?**
  - Servidores, Equipos de Cómputo, Equipos de Comunicación e Información.
- **¿De qué personas se necesita proteger los recursos?**
  - De personas que buscan su beneficio personal, o poder dentro de la institución.
  - De personas deshonestas que cometen sabotaje interno.
  - De personas que roban a la institución.
  - De personas que utilizan la red para transmitir virus o códigos maliciosos.

- **¿Qué tan reales son las amenazas?**
  - La información esta a menudo expuesta a robo, sabotaje, virus, códigos maliciosos, etc.
- **¿Qué tan importantes son los recursos a proteger?**
  - Los servidores y equipos de cómputo guardan la información de la institución, la cual en algunos casos es pública y en otros es confidencial.
  - Sin los Equipos de comunicación no se tendría conexión con las diferentes Áreas de Salud.

Establecer el valor de los datos es algo totalmente relativo, pues la información constituye un recurso que en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, la documentación o las aplicaciones.
Además, las medidas de seguridad no influyen en la productividad del sistema por lo que las organizaciones son resistentes a dedicar recursos a esta tarea. Por eso es importante entender que los esfuerzos invertidos en la seguridad tienen costo.

El objetivo que se persigue es lograr que un ataque a los bienes sea más costoso que su valor, e invirtiendo menos de lo que vale. Para esto se define tres costos fundamentales.

CP: Valor de los bienes y recursos protegidos.

CR: Costo de los medios necesarios para romper las medidas de seguridad establecidas.

CS: Costo de las medidas de seguridad.

Para que la política de seguridad sea lógica y consistente se debe cumplir que:

CR > CP: o sea que un ataque para obtener los bienes debe ser más costoso que el valor de los mismos. Los beneficios obtenidos de romper las medidas de seguridad no deben compensar el costo de desarrollo del ataque.

CP > CS: o sea que el costo de los bienes protegidos debe ser mayor que el costo de la protección.

Por lo tanto:

CR > CP > CS y lo que se busca es:

- Minimizar el costo de la protección manteniéndolo por debajo de los bienes protegidos. Si proteger los bienes es mas caro de lo que valen, entonces resulta más conveniente obtenerlos de nuevo en vez de protegerlo.

- Maximizar el costo de los ataques manteniéndolo por encima del de los bienes protegidos. Si atacar el bien es más caro de lo que valen, al atacante le conviene mas obtenerlo de otra forma menos costosa.

2.4.1.1 Tipos de Costos

2.4.1.1.1 Costo Intrínseco

Consiste en otorgar un valor a la información contestando las preguntas anteriormente expuestas.

2.4.1.1.2 Costo Derivado de la Pérdida

Son todos los valores generados por las Pérdidas de algún componente de los sistemas u otro/s recurso/s y/o elementos de la red.

Para esto se consideró elementos como:(Para el caso de la información)

- Información aparentemente inocua como datos personales, que deben permitir a alguien suplantar identidades.
- Datos confidenciales de acuerdos y contratos que un atacante podría usar paras su beneficio.
- Tiempos necesarios para obtener ciertos bienes. Un atacante podría acceder a ellos para ahorrarse el costo o tiempo necesario para su desarrollo.

2.4.2 MEDIDAS DE PROTECCIÓN

- **Seguridad Física:**

  - Colocar a los equipo en áreas protegidas
  - Deshabilitar cualquier periférico que no se utilice con frecuencia (como disquetera, CDROM, etc.)
  - Proteger el BIOS del equipo con clave
  - Deshabilitar Puertos Seriales y/o Paralelos que no se utilicen con frecuencia.
  - Proteger las laptops con cables de acero.

- Proteger los Servidores en armarios con puertas con seguros para evitar que los servidores sean apagados intencionalmente o por accidente.
- En cada servidor se debe utilizar antivirus de Protección modo Server, actualizarlo o configurarlo para que automáticamente integre las nuevas actualizaciones del propio software y de las definiciones o bases de datos de virus registrados.
- Crear Niveles de Seguridad para permisos para acceso a equipos de comunicaciones administrables (router, switch, Access Point), computadoras o servidores y/o permisos de uso a archivos y de recursos.
- No usar nombres y usuarios predeterminados por los softwares de aplicaciones o de bases de datos.
- En computadoras que utilicen Sistemas Operativos de Microsoft, hay que realizar actualizaciones periódicas, ya que constantemente los Hacker y creadores de virus encuentran vulnerabilidades en dichos sistemas operativos.
- Instalar Software que detecte y remueva "spywares" tanto en los computadores de los usuarios y servidores.
- Ubicar los Access Point en lugares difíciles de acceso para evitar hurtos o sabotajes.
- Ubicar los Access Point preferiblemente en lugares altos en donde posea una buena Transmisión y Recepción de la Señal.
- Establecer políticas rígidas a las personas encargadas de la seguridad del edificio al momento de sacar un equipo de la institución si excepciones ya sean usuarios internos o externos.
- Los equipos que estén dados de baja se deben ser entregados en un plazo máximo de 5 días al Departamento de Bienes y Propiedades para evitar Pérdidas.
- Todos los equipos, computadores y servidores deben estar debidamente etiquetados.
- Los respaldos deben estar situados en un lugar seguro debidamente etiquetado y registrado con el nombre del profesional que lo generó,

fecha, hora, tamaño del archivo, extensión de archivo, y nombre de la base de datos.

- Establecer Políticas de no comer, beber y fumar cerca de los equipos informáticos.
- El perímetro del área de Servidores del PGI, es muy pequeño para el crecimiento continuo de equipos.
- Se debe adquirir UPS para los servidores.
- Cambio de los puntos eléctricos.
- Contar con una instalación eléctrica adecuada, no hay que saturar las tomas de corriente (que es muy común).
- Otorgar ups o reguladores de voltaje a cada equipo informático.
- Los extintores debe ser especiales para equipos informáticos.
- Realizar mantenimiento Preventivo a los equipos informáticos.
- Capacitación permanente a los acerca de Seguridad Física.

- **La seguridad lógica:**

  - Utilización de un sistema operativo relativamente seguro (NT, 2000, UNIX, Linux, etc.).
  - Elección de Passwords seguros.
  - Activado del protector de pantalla con password cuando el equipo queda desatendido y hacer logoff antes de retirarse del mismo.
  - Utilización de un buen firewall.
  - Utilización de antivirus y detectores de troyanos.
  - Utilización de dispositivos de identificación por biométrica (huellas dactilares, escaneo de retina, reconocimiento de voz, etc.).
  - Evitar totalmente usar passwords con nombres de la empresa, departamento o proceso, nombres de usuario o datos personales.
  - Para la generación de passwords realizar combinaciones de letras mayúsculas, minúsculas y números alternadamente.
  - Evitar compartir los passwords.
  - Cambiar periódicamente los passwords de acceso.

- Los passwords de acceso a los sistemas deben ser creados para cada usuario, de acuerdo a los requerimientos del Proceso.
- El password de Administrador solo debe tener acceso máximo dos técnicos del Proceso de Gestión Informática.
- Los Password debe ser registrados en una Bitácora con su fecha de creación, fecha de caducidad y el profesional que lo va a obtener.
- Restringir el acceso a los programas y archivos.
- Asegurar que los usuarios puedan trabajar sin una supervisión minuciosa y constante y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- Identificación y Autentificación de usuarios.
- Roles de usuarios para el caso de bases de datos.
- Obtención de Software de Administración de usuarios en la red, el cual permite limitar el acceso de los usuarios a determinadas horas, zonas, máquinas y sistemas.

➢ **Para Protección contra Hackers:**

- Instalar y mantener actualizado un buen antivirus.
- Instalar y configurar adecuadamente un buen firewall (cortafuegos).
- Instalar todos los parches de seguridad para su sistema operativo.
- Cerrar todos los servicios, excepto los imprescindibles.
- Capacitación permanente acerca de Seguridad Lógica a los técnicos del PGI.

➢ **Seguridad en Comunicaciones:**

- Adquisición de Herramientas de Administración y Monitoreo de los diferentes enlaces de datos.
- Adquisición de Herramientas de Administración y Monitoreo de la red LAN.

- Cambiar el cableado de la red por cableado certificado, y que en el actual se corrija la codificación de colores.
- Establecer mínimo un Administrador de Seguridades.
- Etiquetar todos los dispositivos de comunicación y el Data Center.
- Se deben realizar Mantenimiento mínimo cada año de los equipos de comunicaciones (rack, hubs, routers, switch, Access Point.)
- El cableado de red deben de estar protegidos por conductos o canaletas.
- Los cables de red deben de estar separados de los cables eléctricos para evitar interferencias.

CAPITULO III

En el presente capítulo, se exhibe el desarrollo de la auditoria para la gestión de seguridad de la red física y lógica de la DPSP, metodología empleada, plan de trabajo realizado por el auditor, e informe preliminar de la auditoria realizada.

3 DESARROLLO DE LA AUDITORIA PARA LA GESTIÓN DE SEGURIDAD DE LA RED FÍSICA Y LÓGICA DE LA DPSP.

3.1 OBJETIVO DE LA AUDITORÍA

Conocer el estado actual de las Seguridades de la Red Física y Lógica del PGI de la Dirección Provincial de Salud de Pichincha (DPSP) y plantear procedimientos y sugerencias técnicas para mejorar los procesos que se ejecutan en la Institución.

3.2 ALCANCE DE LA AUDITORIA DE LA GESTIÓN DE SEGURIDADES.

El alcance del desarrollo de esta Auditoria Informática se limitará a la Seguridad de la Red Física y Lógica para el Departamento de Gestión Informática y Sistemas (PGI) de la Dirección Provincial de Salud de Pichincha (DPSP) en la ciudad de Quito.

3.3 DETERMINACIÓN DE LOS PROCESOS Y HERRAMIENTAS PARA EL DESARROLLO DE LA AUDITORIA.

Para el desarrollo de esta auditoria los procesos y herramientas que se han determinado son:

Procesos:

- Formulario de visitas[20] y Hallazgos de Auditoria[21]

Herramientas:

- Cuestionarios[22]
- Entrevistas[23]
- Checklist

[20] ANEXO 6. Formulario de visitas y Hallazgos encontrados
[21] ANEXO 6. Formulario de visitas y Hallazgos encontrados
[22] ANEXO 4. Evaluación de la Seguridad
[23] ANEXO 7. Entrevistas

3.4 METODOLOGÍA A EMPLEARSE EN EL PROCESO DE AUDITORIA INFORMÁTICA

La siguiente figura muestra la metodología que se utilizó en el desarrollo de esta auditoría, la cual ha sido basada en la metodología propuesta por el Ing. MSc. Marck Jaramillo Orellana.

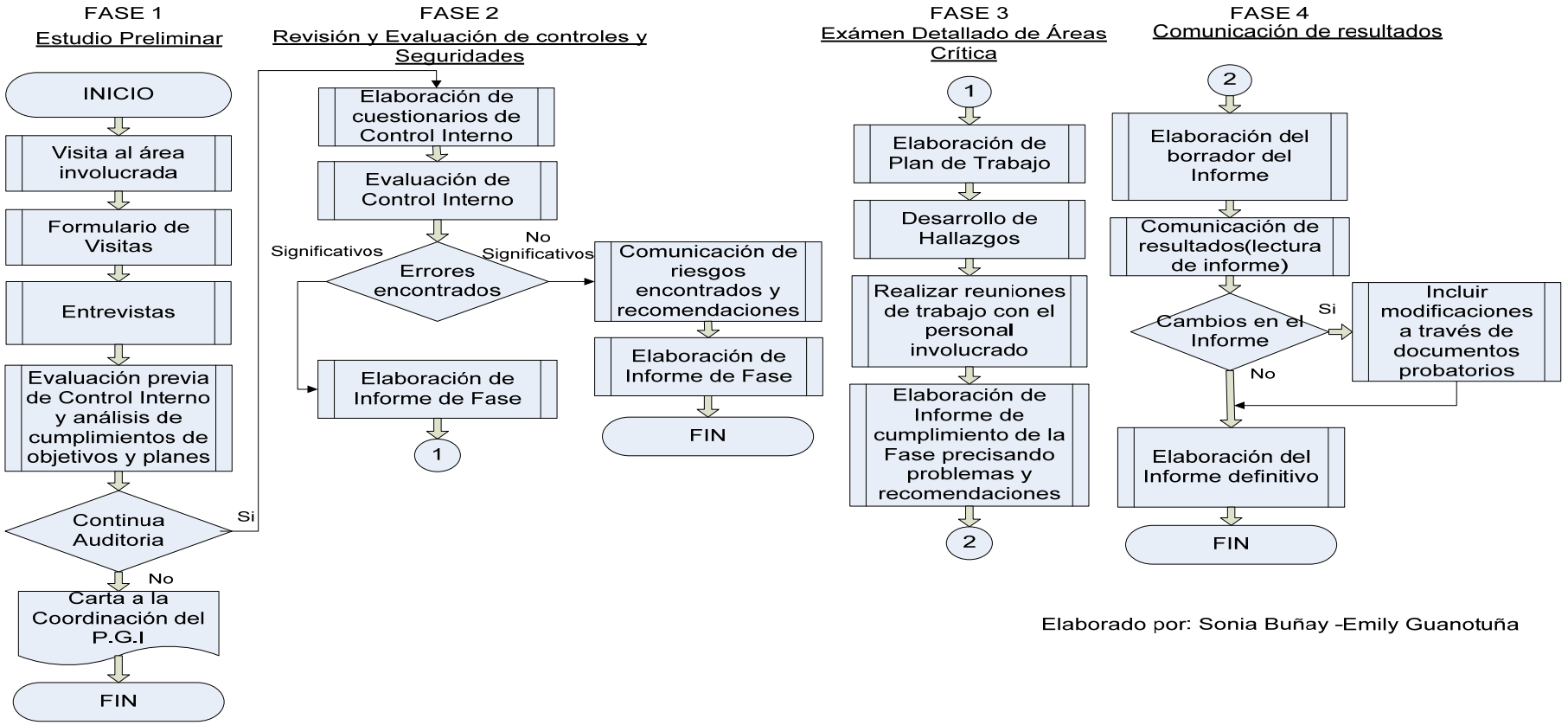


Figura 13.Metodología de la Auditoria

3.5 PLAN DE TRABAJO DE AUDITORIA

En la siguiente figura se muestra el Plan de Trabajo que se ejecutó en la auditoria.

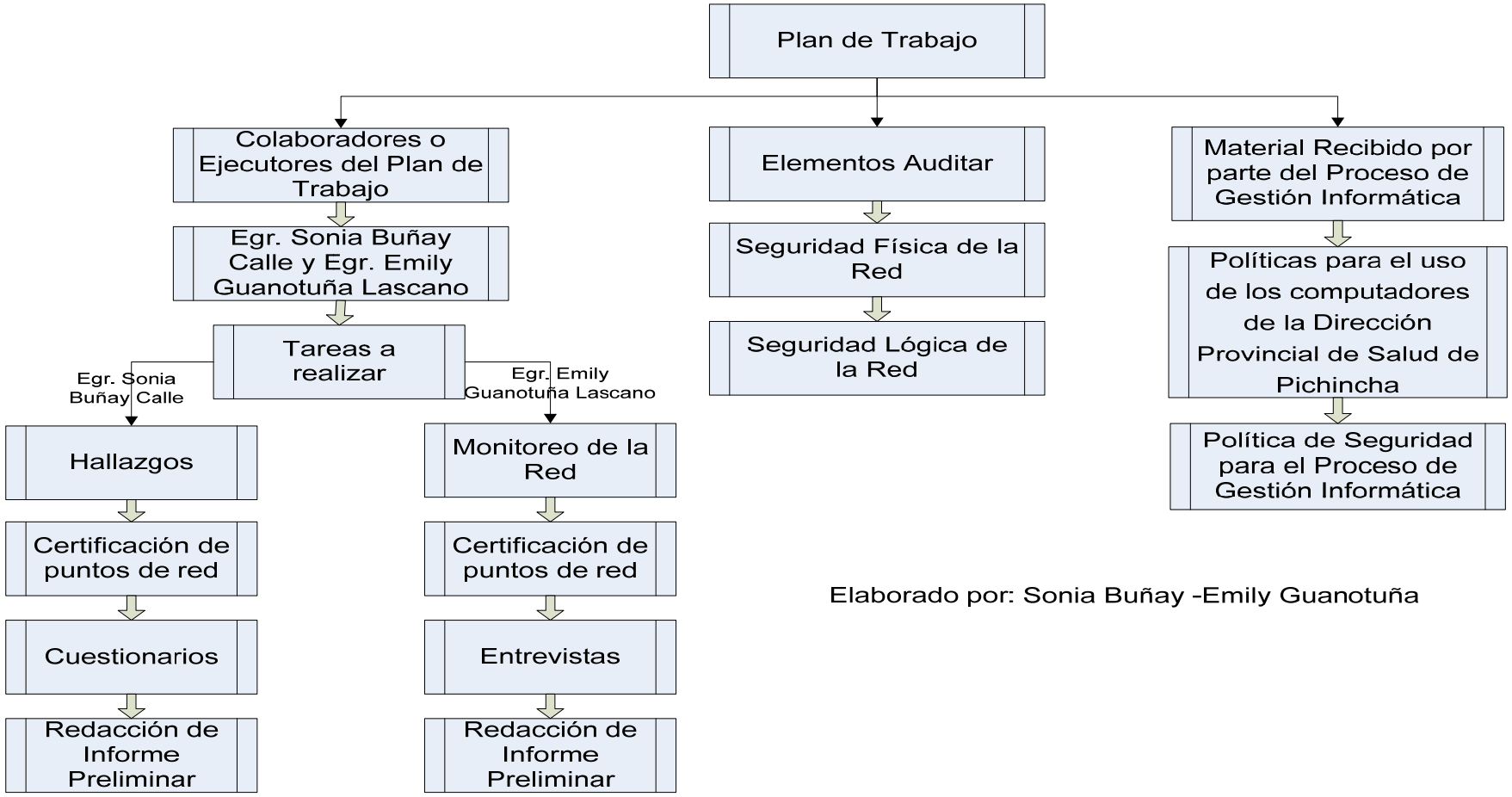


Figura 14.Plan de Trabajo de Auditoria

3.6 AUDITORIA EN CADA UNO DE LOS ÁMBITOS QUE ENGLOBA LA SEGURIDAD DE LA RED.

A continuación, se detalla el informe preliminar con las siguientes anomalías encontradas con respecto a la seguridad de la red lógica y física.

1. **RED FÍSICA**

   En el Proceso de Gestión Informática de la DPSP se encontró las siguientes falencias con respecto a la seguridad física.

Falencia en la Seguridad de:

Hardware

- DataCenter sin ningún estándar de Piso Falso, Control de Accesos, Control de Detección de Incendios según los estándares **TIA/EIA 568-B, TIA/EIA 569-A.**
- Pésima distribución y organización en la instalación de cables de datos y eléctricos en lugares públicos y transitados en la institución.
- Documentación en el que corrobore la existencia de aterrizado de protección del área de comunicaciones, como lo exige la norma **TIA/EIA-607.**
- Inexistencia de CT (Closet de telecomunicaciones) por piso, como lo expresa la norma **TIA/EIA-569-B** que ayuda a reducir la cantidad de Pérdida.
- El sistema de aire acondicionado con el que cuenta el cuarto de servidores, no cumple con lo estipulado, ya que este no se encuentra ambientalmente controlado las 24 horas al día, siete días por semana ni mantiene una temperatura entre 18 y 24 grados centígrados.
- La identificación de cables no cumple con lo estipulado en la norma **TIA/EIA-606.**
- El antivirus actual no cuenta con las licencias suficientes para la cantidad de equipos en la DPSP provocando la infección en todos los equipos y generando inestabilidad en la red.

- No existe un análisis técnico previo del perfil ni de las funciones que los usuarios realizan o realizarán para otorgar los equipos que sean idóneos en su desempeño.
- El proceso de Gestión Informática desconoce el ingreso de nuevo personal a la institución provocando desacierto al momento de entregar un equipo.
- Inexistencia de Parque Informático que especifique el número exacto de equipos y sus características
- No se realiza mantenimiento preventivo a los equipos de cómputo.
- Los toma corrientes del sistema eléctrico del edificio, que están etiquetados como "equipos de cómputo" no soportan la carga de voltaje de las impresoras, copiadoras, escaners[24].

Cuarto de Servidores

En el Proceso de Gestión Informática de la DPSP se encontró las siguientes falencias con respecto a la seguridad en el cuarto de servidores.

En la siguiente figura, se muestra las dimensiones del área física con las que cuenta el Proceso de Gestión Informática y su Cuarto de Servidores.

- Las dimensiones del área física del cuarto de servidores no cumplen con el estándar **TIA-EIA 569,** por el número de usuarios que se tiene en la Institución.
- No cuenta con un sistema de ventilación adecuada.
- No existe señalectica.
- A falta de espacio en el PGI el cuarto de servidores se convierte en bodega.
- No existe identificación de equipos
- El cuarto de servidores no cumple con la norma **TIA/EIA-606**, ya que los ductos de la tubería de aire acondicionado esta sobre los equipos y servidores.

Falencia en la Seguridad de:

[24] Información proporcionada por: Ing. Fredy Nicolalde – Ing. Eléctrico encargado del Sistema Eléctrico en la DPSP

Comunicaciones

En el Proceso de Gestión Informática de la DPSP se encontró las siguientes falencias con respecto a la seguridad en las comunicaciones:

- No disponen de instrumentos para mantenimiento de la red.
- No existe mantenimiento preventivo ni correctivo de los equipos de comunicación(router, switch,)
- No existe el control para el uso y asignación del Internet.
- Constantes caídas de los enlaces.
- No existe un Monitoreo de los Enlaces.
- No existe registro actualizado de módems, controladores, terminales, líneas y todo equipo relacionado con las comunicaciones.
- No existe un registro de asignación de IP para los equipos.

2. RED LÓGICA

En el Proceso de Gestión Informática de la DPSP se encontró las siguientes falencias con respecto a la seguridad lógica.

Falencia en la Seguridad de:

Software

- Inexistencias de Registro de Anomalías de los diferentes Software (Síntomas de problemas y mensajes de error o distintas advertencias).
- El antivirus actual no cuenta con las licencias suficientes para la cantidad de equipos en la DPSP provocando la infección en todos los equipos y generando inestabilidad en la red.
- Falta de control de registro de versiones de actualización de los software´s y/o bases de datos.
- Inexistencias de control de backups y de verificación en la idoneidad del respaldo.
- No existe una correcta y definida administración de las políticas de Internet.
- Falta de control de acceso a los Sistemas y Base de Datos.
- Falta de control en la creación y eliminación de usuarios del correo electrónico en la Institución.

- Inexistencias de etiquetación, control y registro de los backups.
- No existe un cronograma de migración a software libre como lo exige el Registro Oficial 1014.
- No existe un control de los cambios no autorizados en las reglas de seguridad y políticas en los servidores.
- No existe confidencialidad en el manejo de contraseñas de Administrador.
- Usuarios con bajo Nivel Informático
- No existe diccionario de datos de ninguna de las bases de datos implementadas en la institución.
- No existe un inventario de activo, que detalle los recursos de información, ni recursos de software.
- No existe clasificación de información interna de la Institución.
- No existe procedimientos que cumplan con los principios de seguridad informática a red (Disponibilidad, Integridad y Confidencialidad de los datos).

CAPITULO IV

En el presente capítulo, se detalla la elaboración del instructivo a ser implementado en el Proceso de Gestión Informática de la Dirección Provincial de Salud de Pichincha, y los informes presentados por cada fase de la metodología.

4 EJECUCIÓN DEL INSTRUCTIVO DE PROCEDIMIENTOS EN EL PROCESO DE GESTIÓN INFORMÁTICA DE LA DIRECCIÓN PROVINCIAL DE SALUD DE PICHINCHA

Un instructivo de procedimiento de seguridad esta basado en cuatro criterios: Seguridad Organizacional, Seguridad Lógica, Seguridad Física y Seguridad Legal.

Éste instructivo no considerará la Seguridad Legal, ni tampoco la Organizacional por cuanto va hacer ejecutado en el Área de Servidores, y será implementado solo en el PGI.

Además para que un instructivo que se ejecute a nivel de toda la institución debe ser primero aprobado por el Proceso de Asesoría Jurídica e involucrar al Proceso de Recursos Humanos a lo largo de este proceso, y actualmente los lazos de comunicación con estos Procesos de la institución no se encuentran afianzados.

4.1 ELABORACIÓN DEL INSTRUCTIVO DE PROCEDIMIENTOS

El presente instructivo, se crea con el propósito de ayudar a mejorar la Seguridad de la Red Física y Lógica del Departamento de Gestión Informática y Sistemas de la Dirección Provincial de Salud de Pichincha (DPSP).

Este instructivo esta basado en la norma NTP-ISO/IEC 17799:2007 “Código de Buenas Prácticas para la Gestión de la Seguridad de la Información”, compuesto de once dominios o áreas, 39 objetivos de control y 133 controles, los mismos que serán ajustados a las necesidades de la Institución, siendo estas: Seguridad Física y Seguridad Lógica.

En el transcurso del desarrollo de esta auditoria a la fecha del 04 de diciembre del 2009, se dio a conocer de manera extraoficial la existencia de un documento de "POLÍTICAS DE SEGURIDAD PARA EL PROCESO DE GESTIÓN INFORMÁTICA"[25], las cuales no cubren los diferentes ámbitos que el SGSI contempla, es por esta razón que se creó nuevas políticas de seguridad informática.

Las políticas de seguridad informática consisten en asegurar que los recursos del sistema de información (material informático, equipos informáticos o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información ahí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

El Sistema de Gestión de Seguridad Informática (SGSI) garantiza las siguientes características:

- Integridad
- Confidencialidad
- Disponibilidad

POLÍTICAS DE SEGURIDAD

Seguridad Lógica:

El nivel de seguridad lógico debe comprender:

- Administración de Acceso de Usuarios
  - Llevar un registro de la modificación, creación y eliminación de usuarios, tanto como usuarios de correo, como de red.
  - Restringir a los usuarios el acceso a archivos no autorizados.
  - Activado del protector de pantalla con password cuando el equipo quede desatendido y hacer logoff antes de retirarse del mismo.

[25] ANEXO 3. Políticas de Seguridad para el Proceso de Gestión Informática de la DPSP

- Seguridad en Acceso de Terceros
    - Crear usuarios con perfil específico para auditores externos, pasantes, o personal temporal, los mismos que deben ser eliminados una vez terminada su actividad.
- Control de Acceso a la Red
    - Restringir el uso del Internet a usuarios no autorizados
    - Utilizar en modo lectura los recursos de red para prevenir que los equipos de cómputo infectados propaguen el virus.
    - La persona encargada de seguridad debe revisar si se han realizado modificaciones no autorizadas en la configuración del Active Directory.
- Control de Acceso a las Aplicaciones
    - No usar los nombres de bases de datos y/o aplicaciones como nombres de usuarios y password predeterminados.
    - Obtención de logs, para conocer el estado de las aplicaciones o bases de datos ya que estos informan si existen warnings.
    - No compartir cuentas de usuarios entre funcionarios.
    - Crear contraseñas que incluya combinaciones de letras mayúsculas, minúsculas, signos y números.
    - No usar contraseñas que sean de fáciles de asumir(datos personales)
    - Realizar cambios periódicos de contraseñas y registrarlos en una bitácora con fecha de creación, fecha de caducidad y técnico que lo asigna.
    - El password de Administrador de red debe ser conocido únicamente por el Administrador de Red y la persona encargada de Seguridad.
    - Dar permisos a los usuarios que manejan bases de Datos según sus funciones.
- Monitoreo del Acceso y Uso del Sistema
    - No se debe instalar sistemas operativos de estaciones de trabajo en servidores.

- No se debe instalar antivirus de protección de estaciones de trabajo en los servidores.
- Duplicar los instaladores de Bases de Datos, y Herramientas Informáticas.
- Revisar semanalmente que la configuración de actualización de la base de datos de virus este funcionando correctamente.
- Esta prohibido la instalación de programas no autorizados en estaciones de trabajo y servidores.
- Levantar solo los servicios que son necesarios para el funcionamiento del servidor.

- Respaldo de información (servidores, equipos de red)
  - Diariamente sacar backups de todas las bases de datos.
  - Resguardar los backups generados en otro lugar, fuera del PGI.
  - Obtener backups completos, de todos los datos cuando es por primera vez.
  - Realizar pruebas a los backups obtenidos, que demuestre que están en buen estado.
  - Registrar el nombre del profesional que genera los backup, fecha, hora, tamaño del archivo, extensión de archivo, y nombre de la base de datos de la cual se extrajo.

Seguridad Física:

- Colocar a los equipos en áreas protegidas.
- Deshabilitar cualquier periférico que no se utilice con frecuencia (como CD-ROM, USB, DVD-WR.)
- Proteger el BIOS del equipo con clave.
- Deshabilitar Puertos Seriales y/o Paralelos que no se utilicen con frecuencia.
- Proteger las laptops con cables de acero.
- Proteger los Servidores en armarios con puertas con seguros para evitar que los servidores sean apagados intencionalmente o por accidente.
- Ubicar los Access Point en lugares difíciles de accesar para evitar hurtos o sabotajes.

- Ubicar los Access Point preferiblemente en lugares altos en donde posea una buena Transmisión y Recepción de la Señal.
- Controlar el ingreso y egreso de los equipos de cómputo conjuntamente con el Proceso de Servicios Institucionales sin excepciones ya sean usuarios internos o externos.
- Registrar el ingreso, salida y la baja de equipos de cómputo, especificando serie, modelo, marca, usuario responsable, departamento, y en el caso de ser nuevo fecha de adquisición y período de garantía ya sea por partes o piezas.
- Entregar en un plazo máximo de cinco días al Departamento de Bienes y Propiedades los equipos que estén dados de baja.
- Etiquetar debidamente las Impresoras de red (IP, Máscara, Puerta de enlace), Access Points (Nombre del Access Point, SSID, IP, Máscara, Puerta de enlace) y Servidores (Nombre del Servidor, IP, Mascara, Puerta de Enlace).
- Los respaldos deben estar situados en un lugar seguro debidamente etiquetado y registrado con el nombre del profesional que lo generó, fecha, hora, tamaño del archivo, extensión de archivo, y nombre de la base de datos.
- No comer, beber y fumar cerca de los equipos informáticos.
- El uso del UPS es exclusivo para los servidores.
- No utilizar puntos eléctricos que estén en mal estado.
- No saturar los puntos eléctricos conectando varios equipos de cómputo.
- Verificar que todos los equipos informáticos estén conectados a tomas eléctricas etiquetadas como: “equipo de cómputo” o en su defecto a un regulador de voltaje.
- En caso de incendio utilizar los extintores especiales para equipos informáticos(a base de Bióxido de Carbono).
- Cuando se realice mantenimiento Preventivo a los equipos de cómputo registrar lo actuado en cada equipo.

Cuarto de Servidores

- Se prohíbe la introducción de mecheros o elementos con los que se causen fuego.

- En caso de incendio, utilizar el extintor de incendios especial para equipos informáticos(a base de Bióxido de Carbono).
- Ordenar los dispositivos como hubs, routers o switchs.
- Registrarse al ingresar y al salir del cuatro de servidores, indicando la hora de entrada y de salida, describir la actividad que realizó y firma de responsabilidad.
- El ingreso al cuarto de servidores es exclusivo solo para personal autorizado. (Administrador de red y Persona encargado de Seguridad).
- En todo momento debe mantenerse la puerta de ingreso al cuarto de servidores cerrada.
- No modificar la temperatura del aire acondicionado, la misma que se debe mantener en un rango de 10º a 18º centígrados.
- Cumplir con el cronograma de mantenimiento preventivo a los servidores.
- El cuarto de servidores deberá ser de uso exclusivo para servidores, con las debidas seguridades físicas y de acceso.

Seguridad en Comunicaciones:

- Paredes limpias y pintadas de un color claro.
- Todo cambio que se realice en las configuraciones internas de la red(los servidores), y en los dispositivos de comunicación, debe ser documentado, y autorizado por la persona competente.
- Cambios y adiciones de nuevos puntos deben ser documentados y realizados bajo autorización.
- Etiquetar los patch cord y utilizar colores diferentes para identificar los puntos de voz, de los puntos de datos.

4.2 EJECUCIÓN DEL INSTRUCTIVO DE PROCEDIMIENTOS EN EL DEPARTAMENTO DE GESTIÓN DE SISTEMAS E INFORMÁTICA DE LA DPSP DEL ÁREA DE SERVIDORES.

En la ejecución del instructivo se realizaron las siguientes actividades:

- Se entregó formalmente el Instructivo en que constan las Políticas de Seguridad para el Cuarto de Servidores.
- Se reestructuró (Peinado) el cableado estructurado del Cuarto de Servidores.
- Se etiquetó cada uno de los Servidores, con sus respectivos, Nombres, IPs, Máscaras, y Aplicaciones instaladas.
- Se reordenó el espacio físico del Cuarto de Servidores, desalojando cartones, cables, y equipos en estado obsoleto.
- Se reclasificó backups, manuales de las licencias, manuales de office 95 y 98, e instaladores de Sistemas Operativos y Office de estos años y se etiquetó el espacio físico en donde reposarán los mimos.
- Se ubicó avisos de “Prohibido el ingreso a personas no autorizadas”, a la entrada del Cuarto de Servidores.
- Se entregó una plantilla para el registro del ingreso de personal al Cuarto de Servidores, que servirá para controlar las modificaciones que se hacen en los equipos de comunicación y/o servidores, en la plantilla constan los siguientes campos: nombre del técnico, hora & fecha, proceso o acción realizada, nombre del equipo, base de datos y/o software y requerimiento notificado.
- Se entregó una plantilla de registro para el control de respaldos en la cual constan los siguientes campos: nombre del responsable, hora & fecha, nombre del archivo y log, tamaño del archivo, lugar físico & lógico en el que se encuentra el respaldo original y sus copias.
- Se colocó interna y externamente los controles que ayudarán a precautelar la seguridad del Cuarto de Servidores y sus recursos.
- Se certificó seis puntos de red con el equipo certificador ***FLUKE DTX 1800 (UTP).***

Para constancia ver las siguientes figuras:

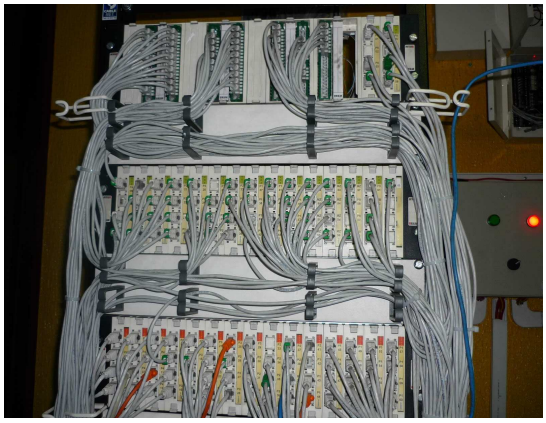


Figura 15. Rack reestructurado.

Figura 16. Etiquetado de Servidores

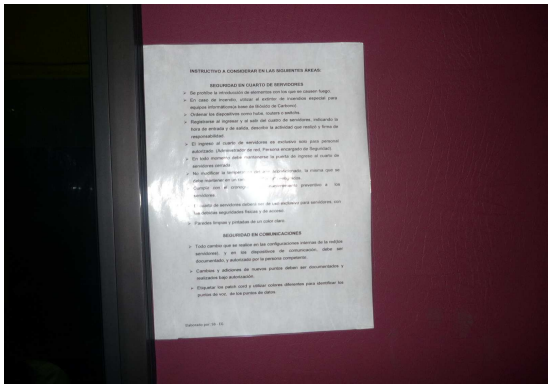


Figura 17. Pimiento de Control de Respaldos

Figura 18. Reclasificación de Licencias, Backups.

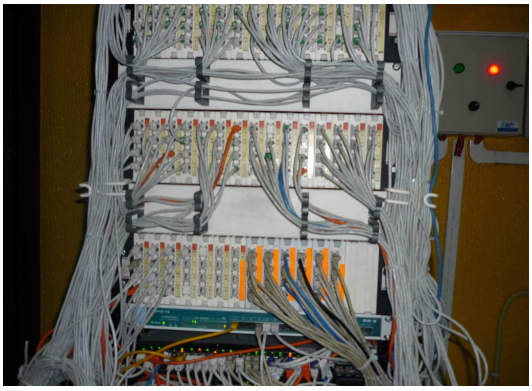


Figura 19. Etiquetado de Patch Panel

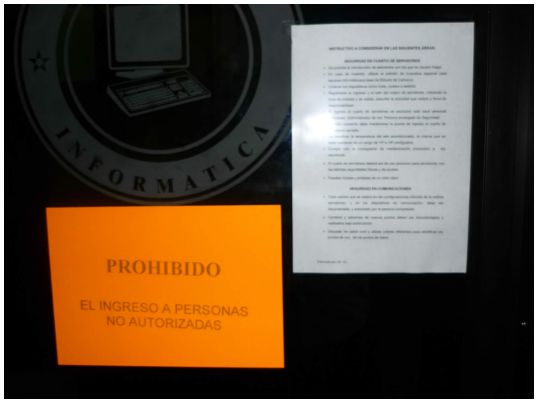


Figura 20. Políticas de Seguridad

Figura 21. Certificación del Cableado Estructurado (Rack-Farmacia)

Figura 22. Certificación de Cableado Estructurado (Estación de Trabajo-Área de Farmacia)

4.3 GENERAR INFORMES Y/O DOCUMENTACIÓN TÉCNICA BASADA EN LOS RESULTADOS

Entrega de Informe de FASE II

Quito, Julio del 2009

Pese a que el Proceso de Gestión Informática (PGI) no cuenta a la fecha con: Plan Estratégico, Plan Orgánico Funcional, Plan Orgánico Estructural que haya sido dado a conocer a todo el equipo personal del PGI, cumpliéndose así con la Fase I que es el estudio preliminar.

Se decide continuar con la Auditoria ejecutando como primer paso la Evaluación de la Seguridad Física de forma general en: Instalaciones eléctricas, aire acondicionado, área de servidores, autorización de accesos, sistemas de incendio, redes y comunicaciones. Como segundo paso la Evaluación de Control Interno a la Seguridad Física y a la Seguridad Lógica del PGI, encontrando falencias en todo lo relacionado a: Accesos al PGI, y al cuarto de servidores.

Con esto se da paso a la propuesta del Plan de Trabajo a elaborarse en la Fase III.

Entrega de Informe de FASE III

Quito, Septiembre del 2009

Se elabora un plan de actividades a seguir, entre las cuales están: la instalación y uso de herramientas como IP Tools, para el monitoreo de la red cableadas Net Stumbler para el monitoreo de la red inalámbrica, además se desarrollaron hallazgos de auditoria, se realizó pruebas de certificación a siete puntos de red, para descartar que la pérdida de señal, sea producto del maltrato del cableado y estas se realizaron con el equipo ***FLUKE DTX 1800 (UTP).***

Por lo tanto, se recomienda:

- Se adquiera nuevos Access Point o Repetidores de Señal, ó en el mejor de los casos se implemente Closets de Telecomunicaciones en cada piso.
- Se adquiera un mejor antivirus.
- Se adquiera herramientas de firewall y antispam.
- Se realice un cronograma para realizar mantenimiento preventivo a todos los equipos de cómputo.
- Se revise normas de cableado estructurado.
- Se proporcione control de seguridad de a los Access Points.
- Se establezcan controles de seguridad para los accesos no autorizados.

Entrega de Informe de FASE IV

Quito, Diciembre del 2009

El informe preliminar o informe de borrador ha sido entregado el 01 de diciembre del 2009 a la Ing. Maritza Badillo Coordinadora del Proceso de Gestión Informática, indicando las novedades encontradas en la Seguridad Física, Seguridad Lógica y Seguridad de Comunicaciones con sus respectivas recomendaciones.

Quedando el informe preliminar a presentar de la siguiente manera:

INFORME PRELIMINAR

Quito 01, diciembre del 2009

Ing. Maritza Badillo
COORDINADORA DEL PROCESO DE GESTIÓN INFORMÁTICA
Presente.

De nuestra consideración:

Yo, Sonia Buñay y Emilly Guanotuña, nos dirigimos a usted para darle a conocer el dictamen preliminar de la Auditoría practicada a la Seguridad de la Red Física y Lógica de la DPSP. La misma que se ha llevado a cabo desde el 04 de mayo al 26 de noviembre del presente año.
De los resultados obtenidos me permito informarle las siguientes observaciones:

1. **RED FÍSICA**
   En el Proceso de Gestión Informática de la DPSP se encontró las siguientes falencias con respecto a la seguridad física.

Falencia en la Seguridad de:
Hardware

- DataCenter sin ningún estándar de Piso Falso, Control de Accesos, Control de Detección de Incendios según los estándares **TIA/EIA 568-B, TIA/EIA 569-A.**
- Pésima distribución y organización en la instalación de cables de datos y eléctricos en lugares públicos y transitados en la institución.
- Documentación en el que corrobore la existencia de aterrizado de protección del área de comunicaciones, como lo exige la norma **TIA/EIA-607.**

- Inexistencia de CT (Closet de telecomunicaciones) por piso, como lo expresa la norma **TIA/EIA-569-B** que ayuda a reducir la cantidad de Pérdida.
- El sistema de aire acondicionado con el que cuenta el cuarto de servidores no cumple con lo estipulado, ya que este no se encuentra ambientalmente controlado las 24 horas al día, siete días por semana ni mantiene una temperatura entre 18 y 24 grados centígrados.
- La identificación de cables no cumple con lo estipulado en la norma **TIA/EIA-606.**
- No existe seguridad física para los equipos, ni personas.
- No existe control de entrada y salida de equipos.
- Mal uso de los recursos informáticos de la Institución.
- El antivirus actual no cuenta con las licencias suficientes para la cantidad de equipos en la DPSP provocando la infección en todos los equipos y generando inestabilidad en la red.
- No existe un análisis técnico previo del perfil ni de las funciones que los usuarios realizan o realizarán para otorgar los equipos que sean idóneos en su desempeño.
- El proceso de Gestión Informática desconoce el ingreso de nuevo personal a la institución provocando desacierto al momento de entregar un equipo.
- Inexistencia de Parque Informático que especifique el número exacto de equipos y sus características
- No existe control de garantía de equipos, periféricos, partes y piezas.
- Pérdidas constantes de energía.
- Equipos que se quedan sin reparación por falta de presupuesto.
- No se realiza un mantenimiento preventivo del Sistema Eléctrico.
- No se realiza mantenimiento preventivo a los equipos de cómputo.
- Los toma corrientes del sistema eléctrico del edificio, que están etiquetados como “equipos de cómputo” no soportan la carga de voltaje de las impresoras, copiadoras, escaners[26].

[26] Información proporcionada por: Ing. Fredy Nicolalde – Ing. Eléctrico encargado del Sistema Eléctrico en la DPSP

Cuarto de Servidores

En el Proceso de Gestión Informática de la DPSP se encontró las siguientes falencias con respecto a la seguridad en el cuarto de servidores.

En la siguiente figura se muestra las dimensiones del área física con las que cuenta el Proceso de Gestión Informática y su cuarto de servidores.

- Las dimensiones del área física del cuarto de servidores no cumplen con el estándar **TIA-EIA 569,** por el número de usuarios que se tiene en la Institución.
- No cuenta con un sistema de ventilación adecuada.
- No existe señalectica.
- A falta de espacio en el PGI el cuarto de servidores se convierte en bodega.
- Actualmente existe un extintor de fuego en el PGI, más no en el cuarto de servidores, este extintor tiene la fecha de vencimiento caducada en marzo del 2009; y este no es para el uso en equipos de cómputo. Además los técnicos desconocen su uso y manejo.
- No existe identificación de equipos
- El cuarto de servidores no cumple con la norma **TIA/EIA-606**, ya que los ductos de la tubería de aire acondicionado esta sobre los equipos y servidores.
- La puerta del cuarto de servidores no cumple con la norma **TIA/EIA-569-B**, por cuanto esta no ofrece la seguridad que el espacio debe tener, ni tampoco cumple con lo propuesto en la norma.

Recomendaciones:

Hardware

De acuerdo a las falencias encontradas con respecto al Hardware, se expone las siguientes recomendaciones:

- Rediseñar un sistema de cableado estructurado tomando en cuenta los estándares **TIA/EIA 568-B-2, TIA/EIA 569-B, TIA/EIA 606A, TIA/EIA 607 y TIA/EIA/TSB-67**

- Las líneas de energía eléctrica y telecomunicaciones que se conectan con las instalaciones de procesamiento de la información deben ser empotradas en la pared o instaladas dentro de canaletas separadas.
- Elaborar el documento en el que se esquematice el diseño de aterrizado de protección, especificando lugar, dimensiones, técnicas y materiales utilizados.
- Proteger a los equipos de los ductos de aire acondicionado, ya que estos sufren constantes desperfectos llegando a congelar el artefacto (aire acondicionado) y sus tuberías.
- Realizar Mantenimiento Preventivo a los aire acondicionados en forma periódica llevando un registro que contenga fecha, descripción de lo realizado, empresa y técnico que lo realizó, y responsable de la DPSP encargado.
- Acordar entre el Proceso de Servicios Institucionales (Bienes y Propiedades) y el Proceso de Gestión Informática para realizar los debidos controles, para los egresos e ingresos de equipos tanto para los usuarios internos como personas ajenas a la institución.
- Se concientice a los usuarios acerca de los recursos que la Institución le proporciona como herramienta de trabajo, que es para la productividad de la misma y no para usos personales.
- Realizar un análisis que identifique y reasigne, si el equipo de cómputo cumple con las necesidades del usuario de acuerdo con sus funciones.
- Solicitar al Proceso de Recursos Humanos realice una coordinación previa con el Proceso de Gestión Informática al momento de realizar la contratación del nuevo personal, para preparar el equipo de cómputo que se asignará al usuario, de acuerdo a las funciones que ejecutará reduciendo así el tiempo de entrega.
- Elaborar y mantener un inventario de los activos importantes asociados a cada sistema de información, cada activo debe ser claramente identificado con su usuario responsable, los activos a inventariar son:

  Activos físicos:

  - Equipamiento informático(CPU, monitores, laptop´s, módems)
  - Equipos de Comunicaciones (routers, máquinas de fax, contestadores automáticos)

- Medios Magnéticos (cintas y discos)
- Equipos Técnicos (suministros de electricidad, unidades de aire acondicionado)
- Mobiliario
- Servicios (aire acondicionado, calefacción, iluminación y energía eléctrica) tomando en cuenta la indicaciones de la **ISO 17799:2007**.

- Crear una Base de Datos, que ayude a controlar las fechas de garantías de los equipos, en la que consten: nombre de la empresa, fecha de adquisición, cantidad, valor, y adicionales por compras.
- Solicitar de manera urgente, al Proceso de Mantenimiento, rediseñe el Sistema Eléctrico ayudando con esto a prolongar la vida útil de los equipos de cómputo y/o servidores; Incluyendo en el rediseño, circuitos adicionales para el cuarto de servidores.
- Se comprometa la Coordinación del PGI con la Institución, organizando de manera acertada las diferentes asignaciones de partidas presupuestarias para los gastos e inversiones de índole tecnológica.
- Realizar mantenimiento preventivo a los equipos de cómputo y periféricos de manera periódica, ya sean estos semestral o anual, evitando así gastos en métodos correctivos, que conlleva más tiempo, más recurso humano, y pérdida de productividad.

Recomendaciones:

Cuarto de Servidores

De acuerdo a las falencias encontradas con respecto al Cuarto de Servidores, se expone las siguientes recomendaciones:

- Readecuar el cuarto de servidores según normas **TIA/EIA-569-B** *(*Estándar de Espacios y Rutas para Telecomunicaciones para edificios comerciales.)
- Instalar un UPS para el DataCenter.
- Se coloque señaletica alrededor y al interior del cuarto de servidores (prohibido fumar, uso de celulares, no ingreso de alimentos y bebidas) y leyendas preventivas (prohibido cambiar la temperatura al aire

acondicionado, prohibido hacer cambios en los servidores sin autorización).

- Se realice una limpieza y eliminar todo tipo de elemento que no concierna al cuarto de servidores y/o funcionamiento de los mismos.
- Adquirir un sistema de detección y extinción de incendios apto para el uso en los equipos de cómputo, o que no sean nocivos para estos, en el caso de una emergencia. Este extintor debe ser colocado al ingreso del cuarto de servidores.
- La Coordinación organice una capacitación para los funcionarios del PGI, acerca del manejo y uso del extintor, ya que en caso de incendio no se sabría como actuar.
- Se identifique de manera clara cada uno de los equipos y dispositivos que se encuentran en el cuarto de servidores.
- Un sistema de Control de Accesos.

Falencia en la Seguridad de:

Comunicaciones

En el Proceso de Gestión Informática de la DPSP se encontró las siguientes falencias con respecto a la seguridad en las comunicaciones:

- No disponen de instrumentos para mantenimiento de la red.
- Inexistencias de Filtros contra Rayos en las Líneas de Comunicación Externa en las áreas de salud.
- No existe mantenimiento preventivo ni correctivo de los equipos de comunicación(Router, Switch, Hubs, Access Point)
- No existe rotulación en los equipos de comunicación (Router, Switch, Hubs, Access Point)
- No existe el control para el uso y asignación del Internet.
- Utilización inapropiada del Internet.
- Constantes caídas de los enlaces.
- No existe un Monitoreo de los Enlaces.
- No existe registro actualizado de módems, controladores, terminales, líneas y todo equipo relacionado con las comunicaciones.
- No existe un registro de asignación de IP para los equipos.
- Inexistencias de Estudio Técnico de Factibilidad para la red inalámbrica

Recomendaciones:

Comunicaciones

De acuerdo a las falencias encontradas con respecto al Cuarto de Servidores, se expone las siguientes recomendaciones:

- Adquirir herramientas necesarias para una correcta administración y mantenimiento de la red.
- Adquirir dispositivos pararrayos para cada área de salud.
- Realizar mantenimiento preventivo a los equipos de comunicación.
- Rotular los equipos de comunicación (Router, Switch, Hubs, Access Point)
- Realizar una evaluación a los usuarios, para identificar si es necesario el uso del Internet, para su efectivo desempeño.
- Elaborar y ejecutar normas de “uso apropiado” del Internet y para el personal del DPSP.
- Establecer políticas de monitoreo de la red.
- Realizar un inventario de los dispositivos de red que identifiquen si pertenecen a la Institución o a los proveedores; y con dichos resultados crear una Base de Datos incluyendo fechas de garantías de los mismos.
- Realizar un registro que permita conocer y controlar la asignación de las IP’s, tanto a computadores de usuarios como a servidores, periféricos y dispositivos de red.
- Rediseñar la red inalámbrica, ubicando los Access Point en lugares estratégicos y analizando los posibles elementos que puedan impedir la propagación de la señal; ubicando en lugares donde la señal no sea interrumpida, caso contrario adquirir otros Access Point.
- Redistribución de equipos de cómputo según el perfil del usuario.

2. RED LÓGICA

En el Proceso de Gestión Informática de la DPSP se encontró las siguientes falencias con respecto a la seguridad lógica.

Falencia en la Seguridad de:

Software

- Inexistencias de Registro de Anomalías de los diferentes Software (Síntomas de problemas y mensajes de error o distintas advertencias).
- El antivirus actual no cuenta con las licencias suficientes para la cantidad de equipos en la DPSP provocando la infección en todos los equipos y generando inestabilidad en la red.
- Falta de control de registro de versiones de actualización de los software´s y/o bases de datos.
- Inexistencias de control de backups y de verificación en la idoneidad del respaldo.
- No existe una herramienta de administración de Internet, canales y red.
- No existe una correcta y definida administración de las políticas de Internet.
- Falta de control de acceso a los Sistemas y Base de Datos.
- Falta de control en la creación y eliminación de usuarios del correo electrónico en la Institución.
- Inexistencias de etiquetación, control y registro de los backups.
- No existen Manuales Técnicos de los Diferentes Sistemas.
- Inexistencias de Licencias del Sistema Operativo para la Mayoría de computadores.
- No existe un cronograma de migración a software libre como lo exige el Registro Oficial 1014.
- No existe un control de los cambios en las reglas de seguridad y políticas en los servidores.
- No existe confidencialidad en el manejo de contraseñas de Administrador.
- Usuarios con bajo Nivel Informático
- No existe diccionarios de ninguna de las bases de datos implementadas en la institución.
- No existe un inventario que detalle los recursos de información, ni recursos de software.
- No existe clasificación de información interna de la Institución.

- No existe procedimientos que cumplan con los principios de Seguridad Informática la red (Disponibilidad, Integridad y Confidencialidad de los datos).

Recomendaciones:

- Registrar las Anomalías de los diferentes Software (Síntomas de problemas y mensajes de error o distintas advertencias), para brindar el apoyo adecuado a los usuarios y precautelar el buen funcionamiento de los Software y/o Base de Datos, como lo indica la norma **ISO 17799:2007**.
- Adquirir licencias de antivirus para cubrir todos los equipos de la red.
- Crear controles y registrar los cambios en las versiones de los Sistemas Operativos, Aplicaciones y/o Base de Datos.
- Crear procedimientos de restauración que verifiquen y prueben periódicamente la confiabilidad en la recuperación de los backups.
- Solicitar al Proceso de Recursos Humanos, coordinación con el PGI, informando cuando un usuario de la DPSP deje de prestar sus servicios, en vista que al no conocer, el servidor de correo se satura ya que los correos de estos usuarios no son descargados, ocupando espacio en disco.
- Adquirir una herramienta que permita administrar el Internet, los canales de datos y la Intranet.
- Establecer políticas de control de accesos proporcionando a cada uno de los técnicos del PGI su ID y password a las Base de Datos y sistemas.
- Crear una política de control de etiquetación, registro y manejo de los backups mediante bitácoras en el cual se establezca: fecha y hora de obtención del respaldo, persona responsable, dispositivos de almacenamiento, número de copias, lugar físico de almacenamiento según lo establecido en la norma **ISO 17799:2007**.
- Solicitar a los proveedores de los diferentes Software implementados, los manuales técnicos y/o de usuarios, como sus diccionarios de datos.
- Justificar el escaso número de licencias de los Sistemas Operativos, ya que se incumple con la Ley de Propiedad Intelectual.

- Iniciar la migración de los Sistemas Operativos conjuntamente con los Sistemas y/o Aplicaciones a software libre decretado por la Presidencia de la Republica del Ecuador en el Registro Oficial Nº. 1014.
- Establecer políticas de control de cambios en las reglas de configuración de los servidores, dispositivos de red, etc.
- Establecer políticas de control en el manejo de contraseñas de Administrador tanto de la red como de los sistemas, sugiriendo que la contraseña de Administrador sea cambiada periódicamente y que sea únicamente conocido por el Coordinador del Proceso de Gestión de Informática quien deberá registrar y documentar todos los cambios realizados en las contraseñas de administrador y sus periodos.
- El departamento de Recursos Humanos encargado de las capacitaciones a los usuarios deberá evaluar si fueron asimilados los conocimientos de dicha capacitación.
- Elaborar y mantener un inventario con los siguiente activos:
    - Recursos de información(bases de datos y archivos, documentación de sistemas , manuales de usuarios, material de capacitación ó de soportes, planes de continuidad, información archivada, sistemas de emergencia para reposición de la información (fallback)
    - Recursos de Software (Software de Aplicaciones, software de sistemas, herramientas de desarrollo y utilitarios). Según lo establecido en la norma **ISO 17799:2007**
- Utilizar pautas de clasificación de la información para señalar la necesidad, la prioridad y los grados de protección, grados de sensibilidad y criticidad
- Realizar procedimientos esenciales para la Institución partiendo desde:
    - Protección de datos y Confidencialidad de la Información personal.
    - Protección de registros y documentos de la Institución.
    - Derechos de Propiedad Intelectual

La auditoría se encuentre enfocada en la Seguridad de la Red. Física y Lógica, no podemos apartarnos de la realidad del PGI, que es la ausencia completa de un:

- Plan Operativo Anual.
    - El Plan Operativo Anual existe pero no se ejecuta en el PGI, ya sea por tema de presupuesto o tema burocrático.
- Plan Estratégico.
    - El Proceso de Gestión Informática, no cuenta con un Plan en el que se definan las actividades y procesos a cumplir dentro de este departamento en un periodo determinado, ya que día a día se atienden las actividades que se presentan en el momento.
- Plan Orgánico Funcional.
    - No existe un documento que especifique los cargos con sus respectivos representantes que hay en el Proceso de Gestión Informática, ni tampoco se les a informado de forma verbal.

      A continuación se tiene los nombres de los técnicos que prestan sus servicios en el PGI:
        - Ing. Maritza Badillo - Coordinadora del Proceso
        - Egr. Sonia Buñay
        - Egr. Xavier Morales
        - Sr. Guillermo Mantilla
        - Sr. Wilson Carvajal
        - Egr. Patricia Jácome
        - Sr. Henry Rosero
        - Licda. Mariana Vergara (Secretaria)
- Plan Orgánico Estructural de la DPSP.
    - No existe un documento, ni tampoco se les ha informado por algún medio al personal técnico del PGI, acerca de cómo esta estructurado el Proceso de Gestión Informática.
- Manual de Procedimientos.
    - No existe un manual de procedimientos, que indique al personal técnico que procesos deben seguirse al realizar:
        - Formateo de Discos(se da formato sin sacar respaldos)
        - No se entrega el Equipo completamente configurado a los usuarios (correos electrónicos, usuario de red, antivirus).
        - Entrega de Equipo a nuevos usuarios.
        - Al formatear un servidor.

        - Cambios en las políticas de los sistemas operativos y/o sistemas.
        - Obtención de respaldos.
        - Control de versiones.
        - Errores de Sistemas.
        - Actualizaciones en los sistemas y/o Base de Datos.
        - Adquirir e implementar nuevos Softwares.
        - Adquirir e implementar nuevos Equipos.
        - Parque Informático.
        - Equipos dados de baja.
        - Equipos en envío a soporte técnico.
- Plan de Contingencia
    - No existe un plan de contingencia que sirva de apoyo en caso de un infortunio.

Nota:

La Ing. Maritza Badillo firma como constancia de que estar de acuerdo con lo encontrado y se compromete a realizar modificaciones.

INFORME FINAL

Una vez acabado el plazo, de dar a conocer las modificaciones a realizarse por parte de la Coordinadora, y no habiendo ningún cambio que efectuar, se prosigue a redactar el Informe Final.

Quito, 08 de enero del 2010

Ing. Maritza Badillo
COORDINADORA DEL PROCESO DE GESTIÓN INFORMÁTICA
Presente.

De nuestra consideración:

Yo, Sonia Buñay y Emilly Guanotuña nos dirigimos a usted para darle a conocer el dictamen final de la Auditoria Informática de la Seguridad de la Red Física y Lógica para el Departamento de Gestión Informática y Sistemas de la Dirección Provincial de Salud de Pichincha (DPSP).
La misma que se ha llevado a cabo desde el 04 de mayo del 2009 al 08 de enero del 2010.
De los resultados obtenidos se informa la siguiente:

- Los passwords de los usuarios cumplen con requisitos básicos de nivel de seguridad según pruebas de software pero todo el personal conoce la contraseña de los demás ya que el formato que usan es la primera inicial de su nombre y dos primeras letras del apellido, seguidas de tres números consecutivos y dos signos de dólar.

Por ejemplo:

Si el usuario se llama: Pepita Pérez quedaría así su contraseña: ppe123$$

Sin más sucesos encontrados se añade el informe preliminar como informe final.

1. RED FÍSICA

En el Proceso de Gestión Informática de la DPSP se encontró las siguientes falencias con respecto a la seguridad física.

Falencia en la Seguridad de:

Hardware

- DataCenter sin ningún estándar de Piso Falso, Control de Accesos, Control de Detección de Incendios según los estándares **TIA/EIA 568-B, TIA/EIA 569-A.**
- Pésima distribución y organización en la instalación de cables de datos y eléctricos en lugares públicos y transitados en la institución.
- Documentación en el que corrobore la existencia de aterrizado de protección del área de comunicaciones, como lo exige la norma **TIA/EIA-607.**
- Inexistencia de CT (Closet de telecomunicaciones) por piso, como lo expresa la norma **TIA/EIA-569-B** que ayuda a reducir la cantidad de Pérdida.
- El sistema de aire acondicionado con el que cuenta el cuarto de servidores no cumple con lo estipulado, ya que este no se encuentra ambientalmente controlado las 24 horas al día, siete días por semana ni mantiene una temperatura entre 18 y 24 grados centígrados.
- La identificación de cables no cumple con lo estipulado en la norma **TIA/EIA-606.**
- No existe seguridad física para los equipos, ni personas.
- No existe control de entrada y salida de equipos.
- Mal uso de los recursos informáticos de la Institución.
- El antivirus actual no cuenta con las licencias suficientes para la cantidad de equipos en la DPSP provocando la infección en todos los equipos y generando inestabilidad en la red.
- No existe un análisis técnico previo del perfil ni de las funciones que los usuarios realizan o realizarán para otorgar los equipos que sean idóneos en su desempeño.

- El proceso de Gestión Informática desconoce el ingreso de nuevo personal a la institución provocando desacierto al momento de entregar un equipo.
- Inexistencia de Parque Informático que especifique el número exacto de equipos y sus características
- No existe control de garantía de equipos, periféricos, partes y piezas.
- Pérdidas constantes de energía.
- Equipos que se quedan sin reparación por falta de presupuesto.
- No se realiza un mantenimiento preventivo del Sistema Eléctrico.
- No se realiza mantenimiento preventivo a los equipos de cómputo.
- Los toma corrientes del sistema eléctrico del edificio, que están etiquetados como "equipos de cómputo" no soportan la carga de voltaje de las impresoras, copiadoras, escaners[27].

Cuarto de Servidores

En el Proceso de Gestión Informática de la DPSP se encontró las siguientes falencias con respecto a la seguridad en el cuarto de servidores.

En la siguiente figura se muestra las dimensiones del área física con las que cuenta el Proceso de Gestión Informática y su cuarto de servidores.

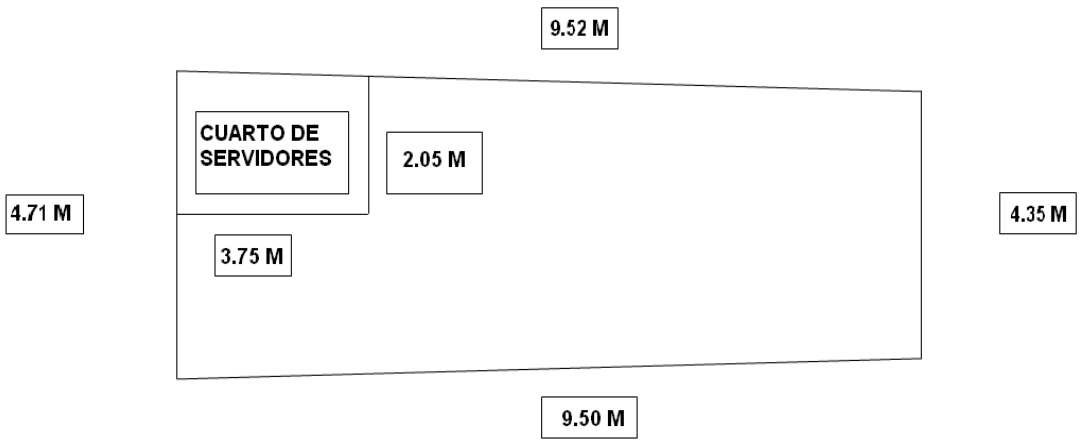


Figura 23. Dimensiones del área física del cuarto de servidores[28]

[27] Información proporcionada por: Ing. Fredy Nicolalde – Ing. Eléctrico encargado del Sistema Eléctrico en la DPSP
[28] Realizado por: Egr. Sonia Buñay – Egr. Emilly Guanotuña

- Las dimensiones del área física del cuarto de servidores no cumplen con el estándar **TIA-EIA 569,** por el número de usuarios que se tiene en la Institución.
- No cuenta con un sistema de ventilación adecuada.
- No existe señalectica.
- A falta de espacio en el PGI el cuarto de servidores se convierte en bodega.
- Actualmente existe un extintor de fuego en el PGI, más no en el cuarto de servidores, este extintor tiene la fecha de vencimiento caducada en marzo del 2009; y este no es para el uso en equipos de cómputo. Además los técnicos desconocen su uso y manejo.
- No existe identificación de equipos
- El cuarto de servidores no cumple con la norma **TIA/EIA-606**, ya que los ductos de la tubería de aire acondicionado esta sobre los equipos y servidores.
- La puerta del cuarto de servidores no cumple con la norma **TIA/EIA-569-B**, por cuanto esta no ofrece la seguridad que el espacio debe tener, ni tampoco cumple con lo propuesto en la norma.

Recomendaciones:

Hardware

De acuerdo a las falencias encontradas con respecto al Hardware, se expone las siguientes recomendaciones:

- Rediseñar un sistema de cableado estructurado tomando en cuenta los estándares **TIA/EIA 568-B-2, TIA/EIA 569-B, TIA/EIA 606A, TIA/EIA 607 y TIA/EIA/TSB-67**
- Las líneas de energía eléctrica y telecomunicaciones que se conectan con las instalaciones de procesamiento de la información deben ser empotradas en la pared o instaladas dentro de canaletas separadas.
- Elaborar el documento en el que se esquematice el diseño de aterrizado de protección, especificando lugar, dimensiones, técnicas y materiales utilizados.

- Proteger a los equipos de los ductos de aire acondicionado, ya que estos sufren constantes desperfectos llegando a congelar el artefacto (aire acondicionado) y sus tuberías.
- Realizar Mantenimiento Preventivo a los aire acondicionados en forma periódica llevando un registro que contenga fecha, descripción de lo realizado, empresa y técnico que lo realizó, y responsable de la DPSP encargado.
- Acordar entre el Proceso de Servicios Institucionales (Bienes y Propiedades) y el Proceso de Gestión Informática para realizar los debidos controles, para los egresos e ingresos de equipos tanto para los usuarios internos como personas ajenas a la institución.
- Se concientice a los usuarios acerca de los recursos que la Institución le proporciona como herramienta de trabajo, que es para la productividad de la misma y no para usos personales.
- Realizar un análisis que identifique y reasigne, si el equipo de cómputo cumple con las necesidades del usuario de acuerdo con sus funciones.
- Solicitar al Proceso de Recursos Humanos realice una coordinación previa con el Proceso de Gestión Informática al momento de realizar la contratación del nuevo personal, para preparar el equipo de cómputo que se asignará al usuario, de acuerdo a las funciones que ejecutará reduciendo así el tiempo de entrega.
- Elaborar y mantener un inventario de los activos importantes asociados a cada sistema de información, cada activo debe ser claramente identificado con su usuario responsable, los activos a inventariar son:

  Activos físicos:

  - Equipamiento informático(CPU, monitores, laptop´s, módems)
  - Equipos de Comunicaciones (routers, máquinas de fax, contestadores automáticos)
  - Medios Magnéticos (cintas y discos)
  - Equipos Técnicos (suministros de electricidad, unidades de aire acondicionado)
  - Mobiliario

- Servicios (aire acondicionado, calefacción, iluminación y energía eléctrica) tomando en cuenta la indicaciones de la **ISO 17799:2007**.

- Crear una Base de Datos, que ayude a controlar las fechas de garantías de los equipos, en la que consten: nombre de la empresa, fecha de adquisición, cantidad, valor, y adicionales por compras.
- Solicitar de manera urgente, al Proceso de Mantenimiento, rediseñe el Sistema Eléctrico ayudando con esto a prolongar la vida útil de los equipos de cómputo y/o servidores; Incluyendo en el rediseño, circuitos adicionales para el cuarto de servidores.
- Se comprometa la Coordinación del PGI con la Institución, organizando de manera acertada las diferentes asignaciones de partidas presupuestarias para los gastos e inversiones de índole tecnológica.
- Realizar mantenimiento preventivo a los equipos de cómputo y periféricos de manera periódica, ya sean estos semestral o anual, evitando así gastos en métodos correctivos, que conlleva más tiempo, más recurso humano, y pérdida de productividad.

Recomendaciones:

Cuarto de Servidores

De acuerdo a las falencias encontradas con respecto al Cuarto de Servidores, se expone las siguientes recomendaciones:

- Readecuar el cuarto de servidores según normas **TIA/EIA-569-B** *(*Estándar de Espacios y Rutas para Telecomunicaciones para edificios comerciales.)
- Instalar un UPS para el DataCenter.
- Se coloque señaletica alrededor y al interior del cuarto de servidores (prohibido fumar, uso de celulares, no ingreso de alimentos y bebidas) y leyendas preventivas (prohibido cambiar la temperatura al aire acondicionado, prohibido hacer cambios en los servidores sin autorización).
- Se realice una limpieza y eliminar todo tipo de elemento que no concierna al cuarto de servidores y/o funcionamiento de los mismos.

- Adquirir un sistema de detección y extinción de incendios aptos para el uso en los equipos de cómputo, o que no sean nocivos para estos, en el caso de una emergencia. Este extintor debe ser colocado al ingreso del cuarto de servidores.
- La Coordinación organice una capacitación para los funcionarios del PGI, acerca del manejo y uso del extintor, ya que en caso de incendio no se sabría como actuar.
- Se identifique de manera clara cada uno de los equipos y dispositivos que se encuentran en el cuarto de servidores.
- Un sistema de Control de Accesos.

Falencia en la Seguridad de:

Comunicaciones

En el Proceso de Gestión Informática de la DPSP se encontró las siguientes falencias con respecto a la seguridad en las comunicaciones:

- No disponen de instrumentos para mantenimiento de la red.
- Inexistencias de Filtros contra Rayos en las Líneas de Comunicación Externa en las áreas de salud.
- No existe mantenimiento preventivo ni correctivo de los equipos de comunicación(Router, Switch, Hubs, Access Point)
- No existe rotulación en los equipos de comunicación (Router, Switch, Hubs, Access Point)
- No existe el control para el uso y asignación del Internet.
- Utilización inapropiada del Internet.
- Constantes caídas de los enlaces.
- No existe un Monitoreo de los Enlaces.
- No existe registro actualizado de módems, controladores, terminales, líneas y todo equipo relacionado con las comunicaciones.
- No existe un registro de asignación de IP para los equipos.
- Inexistencias de Estudio Técnico de Factibilidad para la red inalámbrica

Recomendaciones:

Comunicaciones

De acuerdo a las falencias encontradas con respecto al Cuarto de Servidores, se expone las siguientes recomendaciones:

- Adquirir herramientas necesarias para una correcta administración y mantenimiento de la red.
- Adquirir dispositivos pararrayos para cada área de salud.
- Realizar mantenimiento preventivo a los equipos de comunicación.
- Rotular los equipos de comunicación (Router, Switch, Hubs, Access Point)
- Realizar una evaluación a los usuarios, para identificar si es necesario el uso del Internet, para su efectivo desempeño.
- Elaborar y ejecutar normas de “uso apropiado” del Internet y para el personal del DPSP.
- Establecer políticas de monitoreo de la red.
- Realizar un inventario de los dispositivos de red que identifiquen si pertenecen a la Institución o a los proveedores; y con dichos resultados crear una Base de Datos incluyendo fechas de garantías de los mismos.
- Realizar un registro que permita conocer y controlar la asignación de las IP’s, tanto a computadores de usuarios como a servidores, periféricos y dispositivos de red.
- Rediseñar la red inalámbrica, ubicando los Access Point en lugares estratégicos y analizando los posibles elementos que puedan impedir la propagación de la señal; ubicando en lugares donde la señal no sea interrumpida, caso contrario adquirir otros Access Point.
- Redistribución de equipos de cómputo según el perfil del usuario.

2. RED LÓGICA

En el Proceso de Gestión Informática de la DPSP se encontró las siguientes falencias con respecto a la seguridad lógica.

Falencia en la Seguridad de:

Software

- Inexistencias de Registro de Anomalías de los diferentes Software (Síntomas de problemas y mensajes de error o distintas advertencias).

- El antivirus actual no cuenta con las licencias suficientes para la cantidad de equipos en la DPSP provocando la infección en todos los equipos y generando inestabilidad en la red.
- Falta de control de registro de versiones de actualización de los software´s y/o bases de datos.
- Inexistencias de control de backups y de verificación en la idoneidad del respaldo.
- No existe una herramienta de administración de Internet, canales y red.
- No existe una correcta y definida administración de las políticas de Internet.
- Falta de control de acceso a los Sistemas y Base de Datos.
- Falta de control en la creación y eliminación de usuarios del correo electrónico en la Institución.
- Inexistencias de etiquetación, control y registro de los backups.
- No existen Manuales Técnicos de los Diferentes Sistemas.
- Inexistencias de Licencias del Sistema Operativo para la Mayoría de computadores.
- No existe un cronograma de migración a software libre como lo exige el Registro Oficial 1014.
- No existe un control de los cambios en las reglas de seguridad y políticas en los servidores.
- No existe confidencialidad en el manejo de contraseñas de Administrador.
- Usuarios con bajo Nivel Informático
- No existe diccionarios de ninguna de las bases de datos implementadas en la institución.
- No existe un inventario que detalle los recursos de información, ni recursos de software.
- No existe clasificación de información interna de la Institución.
- No existe procedimientos que cumplan con los principios de Seguridad Informática la red (Disponibilidad, Integridad y Confidencialidad de los datos).

Recomendaciones:

- Registrar las Anomalías de los diferentes Software (Síntomas de problemas y mensajes de error o distintas advertencias), para brindar el apoyo adecuado a los usuarios y precautelar el buen funcionamiento de los Software y/o Base de Datos, como lo indica la norma **ISO 17799:2007**.
- Adquirir licencias de antivirus para cubrir todos los equipos de la red.
- Crear controles y registrar los cambios en las versiones de los Sistemas Operativos, Aplicaciones y/o Base de Datos.
- Crear procedimientos de restauración que verifiquen y prueben periódicamente la confiabilidad en la recuperación de los backups.
- Solicitar al Proceso de Recursos Humanos, coordinación con el PGI, informando cuando un usuario de la DPSP deje de prestar sus servicios, en vista que al no conocer, el servidor de correo se satura ya que los correos de estos usuarios no son descargados, ocupando espacio en disco.
- Adquirir una herramienta que permita administrar el Internet, los canales de datos y la Intranet.
- Establecer políticas de control de accesos proporcionando a cada uno de los técnicos del PGI su ID y password a las Base de Datos y sistemas.
- Crear una política de control de etiquetación, registro y manejo de los backups mediante bitácoras en el cual se establezca: fecha y hora de obtención del respaldo, persona responsable, dispositivos de almacenamiento, número de copias, lugar físico de almacenamiento según lo establecido en la norma **ISO 17799:2007**.
- Solicitar a los proveedores de los diferentes Software implementados, los manuales técnicos y/o de usuarios, como sus diccionarios de datos.
- Justificar el escaso número de licencias de los Sistemas Operativos, ya que se incumple con la Ley de Propiedad Intelectual.
- Iniciar la migración de los Sistemas Operativos conjuntamente con los Sistemas y/o Aplicaciones a software libre decretado por la Presidencia de la Republica del Ecuador en el Registro Oficial Nº. 1014.
- Establecer políticas de control de cambios en las reglas de configuración de los servidores, dispositivos de red, etc.

- Establecer políticas de control en el manejo de contraseñas de Administrador tanto de la red como de los sistemas, sugiriendo que la contraseña de Administrador sea cambiada periódicamente y que sea únicamente conocido por el Coordinador del Proceso de Gestión de Informática quien deberá registrar y documentar todos los cambios realizados en las contraseñas de administrador y sus periodos.
- El departamento de Recursos Humanos encargado de las capacitaciones a los usuarios deberá evaluar si fueron asimilados los conocimientos de dicha capacitación.
- Elaborar y mantener un inventario con los siguiente activos:
    - Recursos de información(bases de datos y archivos, documentación de sistemas , manuales de usuarios, material de capacitación ó de soportes, planes de continuidad, información archivada, sistemas de emergencia para reposición de la información (fallback)
    - Recursos de Software (Software de Aplicaciones, software de sistemas, herramientas de desarrollo y utilitarios). Según lo establecido en la norma **ISO 17799:2007**
- Utilizar pautas de clasificación de la información para señalar la necesidad, la prioridad y los grados de protección, grados de sensibilidad y criticidad
- Realizar procedimientos esenciales para la Institución partiendo desde:
    - Protección de datos y Confidencialidad de la Información personal.
    - Protección de registros y documentos de la Institución.
    - Derechos de Propiedad Intelectual

La auditoría se encuentre enfocada en la Seguridad de la Red. Física y Lógica, no podemos apartarnos de la realidad del PGI, que es la ausencia completa de un:

- Plan Operativo Anual.
    - El Plan Operativo Anual existe pero no se ejecuta en el PGI, ya sea por tema de presupuesto o tema burocrático.
- Plan Estratégico.

- El Proceso de Gestión Informática, no cuenta con un Plan en el que se definan las actividades y procesos a cumplir dentro de este departamento en un periodo determinado, ya que día a día se atienden las actividades que se presentan en el momento.

- Plan Orgánico Funcional.
  - No existe un documento que especifique los cargos con sus respectivos representantes que hay en el Proceso de Gestión Informática, ni tampoco se les a informado de forma verbal.

    A continuación se tiene los nombres de los técnicos que prestan sus servicios en el PGI:
    - Ing. Maritza Badillo - Coordinadora del Proceso
    - Egr. Sonia Buñay
    - Egr. Xavier Morales
    - Sr. Guillermo Mantilla
    - Sr. Wilson Carvajal
    - Egr. Patricia Jácome
    - Sr. Henry Rosero
    - Licda. Mariana Vergara (Secretaria)
- Plan Orgánico Estructural de la DPSP.
  - No existe un documento, ni tampoco se les ha informado por algún medio al personal técnico del PGI, acerca de cómo esta estructurado el Proceso de Gestión Informática.
- Manual de Procedimientos.
  - No existe un manual de procedimientos, que indique al personal técnico que procesos deben seguirse al realizar:
    - Formateo de Discos(se da formato sin sacar respaldos)
    - No se entrega el Equipo completamente configurado a los usuarios (correos electrónicos, usuario de red, antivirus).
    - Entrega de Equipo a nuevos usuarios.
    - Al formatear un servidor.
    - Cambios en las políticas de los sistemas operativos y/o sistemas.
    - Obtención de respaldos.
    - Control de versiones.

- Errores de Sistemas.
- Actualizaciones en los sistemas y/o Base de Datos.
- Adquirir e implementar nuevos Softwares.
- Adquirir e implementar nuevos Equipos.
- Parque Informático.
- Equipos dados de baja.
- Equipos en envío a soporte técnico.

- Plan de Contingencia
  - No existe un plan de contingencia que sirva de apoyo en caso de un infortunio.

CAPITULO V

5 CONCLUSIONES Y RECOMENDACIONES

Conclusiones:

- El presente trabajo realizado en la DPSP reveló la situación en la que se encuentra, no siendo ésta la más óptima para el PGI(Proceso de Gestión Informática), ya que se conoció que tienen ausencia total de controles de seguridad.
- Una vez aplicado el análisis de riesgos a los recursos de la Institución, se pudo conocer las amenazas, vulnerabilidades, que probabilidades hay de que ocurra, el nivel de riesgo al que esta sujeto los recursos informáticos de la DPSP y el nivel de impacto que ocasionaría.
- El Proceso de Gestión Informática no cumple con los principios de seguridad informática que son: Disponibilidad, Integridad y Confidencialidad de los diferentes recursos informáticos que la DPSP mantiene.
- Para que la seguridad física y lógica del PGI (Proceso de Gestión Informática) sea consistente, se debe basar en el objetivo principal del análisis de la evaluación de costos, el cual expone lo siguiente: que los medios necesarios que se utilicen para romper las seguridades establecidas (terceras personas) deben ser mayores que: el valor de los bienes y recursos protegidos, y estos deben ser mayor al costo de las medidas de seguridad.
- Los hallazgos de auditoria, cuestionarios de control interno, y entrevistas han sido herramientas apropiadas para la obtención de resultados que muestran las falencias en seguridad a ser consideradas por el PGI (Proceso de Gestión Informática).
- Se presentó un instructivo para la seguridad en el cuarto de servidores, en el cual consta, políticas de seguridad a ser consideradas al momento de ejecutar ciertos procedimientos de relevancia para el PGI (Proceso de Gestión Informática); como también se realizó el reordenamiento del cableado estructurado,

etiquetación de los servidores, clasificación de los materiales (licencias de software, CDs de respaldos, manuales de ofimática) con que cuenta el PGI (Proceso de Gestión Informática).

- La norma ISO 17799:2007 (Código de Buenas Prácticas para la Gestión de la Seguridad de la Información) es idónea para el análisis de la seguridad física y la seguridad lógica ya que establece diez dominios de control que cubren (*casi*) por completo la Gestión de la Seguridad de la Información.

Recomendaciones:

- El presente trabajo puede ser utilizado como modelo para aquellas personas que estén interesadas en realizar una auditoria informática de cualquier tipo, ya que está basada en estándares tanto para el análisis de los riesgos, como para la evaluación de las falencias de seguridad.
- El estándar NIST se debe utilizar para el análisis de riesgo, ya que este procedimiento se utiliza para ejecutar de forma sistemática los riesgos identificados.
- Mantener actualizado los registros de los recursos informáticos para decisiones oportunas.
- Considerar la norma ISO 17799:2007 (Código de Buenas Prácticas para la Gestión de la Seguridad de la Información) para la creación de controles de seguridad.
- Asesorar y transmitir cultura sobre los riegos informáticos, a los que la DPSP esta expuesta.
- Generar procedimientos que guíen a los técnicos del PGI a realizar actividades que garanticen la seguridad de los recursos informáticos de la DPSP.
- Establecer un manual de procedimientos que se encuentren definidos acorde a la misión del PGI (Proceso de Gestión Informática) para garantizar la calidad del servicio que el mencionado Proceso brinda.

GLOSARIO DE TÉRMINOS

Access Point: Es de un dispositivo utilizado en redes inalámbricas de área local (WLAN - Wireless Local Área Network). El Access Point entonces se encarga de ser una puerta de entrada a la red inalámbrica en un lugar específico y para una cobertura de radio determinada, para cualquier dispositivo que solicite acceder, siempre y cuando esté configurado y tenga los permisos necesarios.

Red Inalámbrica: Es aquella que cuenta con una interconexión de computadoras relativamente cercanas, sin necesidad de cables, estas redes funcionan a base de ondas de radio específicas.

Activo: Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Administración: Es conducción racional de actividades, esfuerzos y recursos.

Amenaza: Es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Ataque: Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Auditoria: Es un examen crítico que se realiza con el fin de evaluar la eficacia y eficiencia de una sección, un organismo ó una entidad.

Comunicaciones: Es el proceso de comunicar información en forma binaria entre dos o más puntos.

CPU: Abreviatura de **Central Processing Unít** (Unidad de Proceso Central), la CPU es el cerebro del ordenador, es donde se producen la mayoría de los cálculos; por ende la CPU es el elemento más importante de un sistema informático.

Datos: Datos son los hechos que describen sucesos y entidades. La importancia de los datos está en su capacidad de asociarse dentro de un contexto para convertirse en información.

Dominio: Se basan en el plan de direccionamiento, contienen definiciones del tipo de la organización a la que pertenece el ordenador (educativa, comercial, militar, etc).

DPSP: Dirección Provincial de Salud de Pichincha.

Efectividad: Logro de los objetivos al menor costo y con el menor número de consecuencias imprevistas. Se relaciona con el impacto de las acciones de la organización.

Eficiencia: Logro de los objetivos previamente establecidos, utilizando un mínimo de recursos.

Emisor: Dispositivo que transmite los datos.

Enlace de Datos: Conjunto de los medios utilizados para transmitir entre dos puntos designados una señal digital que tiene una velocidad binaria nominal especificada.

Enlace de Radio: Se denomina radio enlace a cualquier interconexión entre los terminales de telecomunicaciones efectuados por ondas electromagnéticas.

Errores: Es el resultante de aplicar procedimientos, esquemas, algoritmos o reglas que no pueden aplicarse a un problema concreto por no cumplirse las condiciones necesarias mínimas bajo las cuales los procedimientos aplicados conducen a una respuesta con sentido.

Gestión: Se define como la ejecución y el monitoreo de los mecanismos, las acciones y las medidas necesarias para la consecución de los objetivos de la institución.

Hardware: Hace referencia a cualquier componente físico tecnológico, que trabaja o interactúa de algún modo con la computadora. No sólo incluye elementos internos como el disco duro, CD-ROM, disquetera, sino que también hace referencia al cableado, circuitos, gabinete, etc. E incluso hace referencia a elementos externos como la impresora, el Mouse, el teclado, el monitor y demás periféricos.

Herramienta: Es un instrumento con el que se trabaja, que se opera de forma manual. El desarrollo de la tecnología ha logrado que las herramientas se perfeccionen. También se ha trasladado este término a los instrumentos que

tiene un programa o software y que ejecuta diferentes acciones que ayudan a realizar una tarea.

Impacto: Medir la consecuencia al materializarse una amenaza.

Informática: Es la ciencia que estudia el tratamiento automático y racional de la información." Se dice que el tratamiento es automático por ser máquinas las que realizan los trabajos de captura, proceso y presentación de la información, y se habla de racional por estar todo el proceso definido a través de programas que siguen el razonamiento humano.

IP: Serie de números asociadas a un dispositivo (generalmente una computadora), con la cual es posible identificarlo dentro de una red configurada específicamente para utilizar este tipo de direcciones (una red configurada con el protocolo IP - Internet Protocol).

ISO/IEC 17799:2007: Código de Buenas Prácticas para la Gestión de Seguridad de la Información.

Medio: Consiste en el recorrido de los datos desde el origen hasta su destino.

Mensaje: Lo conforman los datos a ser transmitidos.

Monitor: El monitor es un periférico de salida en el que se hace visible al usuario la información que se encuentra dentro de la computadora. Los más comunes suelen ser los que tienen tubos de rayos catódicos (CRT), aunque en la actualidad está aumentando la utilización de los que se basan en las tecnologías LCD y plasma.

Negligencia: Es la falta de actuación dada por simple falta de atención, y privación de importancia en el asunto.

NTP: Norma Técnica Peruana.

PGI: Proceso de Gestión Informática.

Proceso: Es un conjunto de actividades o eventos (coordinados u organizados) que se realizan o suceden (alternativa o simultáneamente) con un fin determinado. Este término tiene significados diferentes según la rama de la ciencia o la técnica en que se utilice.

Recursos: En informática, los recursos son las aplicaciones, herramientas, dispositivos (periféricos).

Red Física: Conjunto formado por dos o más nodos conectados a un mismo medio o canal de comunicación.

Red Lógica: Se refiere en si a todos los protocolos que requiere una red para estar en funcionamiento.

Redes: Están formadas por conexiones entre grupos de computadoras y dispositivos asociados que permiten a los usuarios la transferencia electrónica de información.

Riesgo: El riesgo es la probabilidad de que una amenaza se convierta en un desastre.

Seguridad: Técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados.

SGSI.- Sistema de Gestión de Seguridad Informática.

Sistema Operativo: Conjunto de programas que se integran con el hardware para facilitar al usuario, el aprovechamiento de los recursos disponibles.

Sistema: Es un conjunto de partes o elementos organizadas y relacionadas que interactúan entre sí para lograr un objetivo. Los sistemas reciben (entrada) datos, energía o materia del ambiente y proveen (salida) información, energía o materia.

Sistemas informáticos: Es un conjunto de partes que funcionan relacionándose entre sí con un objetivo preciso. Sus partes son: hardware, software y las personas que lo usan.

Software: Es el equipamiento lógico e intangible de un ordenador. En otras palabras, el concepto de software abarca a todas las aplicaciones informáticas, como los procesadores de textos, las planillas de cálculo y los editores de imágenes.

Topología de red: Se llama topología de una Red al patrón de conexión entre sus nodos, es decir, a la forma en que están interconectados los distintos nodos que la forman.

Usuario: Es un individuo que utiliza una computadora, sistema operativo, servicio o cualquier sistema informático.

Virus: Es un código malicioso que tiene por objeto alterar el normal funcionamiento del computador, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los

datos almacenados en un computador, aunque también existen otros más "benignos", que solo se caracterizan por ser molestos.

Vulnerabilidad: Hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

REFERENCIAS BIBLIOGRAFICAS

WEBGRAFÍA:

- http://groups.google.com.mx/group/lc-ucv-fi/web/leccin-7-el-texto-instructivo
- http://itcp-cerbesa.blogspot.com/2006/10/seguridad-it-parte-2-aspectos-para.html
- http://www.regiolinux.net/cgi-bin/index.cgi?action=static&id=1
- http://www.monografias.com/trabajos32/auditoria-seguridad-informatica/auditoria-seguridad-informatica.shtml
- http://www.microsoft.com/spain/empresas/seguridad/articulos/plan_seguridad.mspx
- http://www.w3.org.
- http://www.microsoft.com/latam/athome/security/privacy/password_checker.mspx

BIBLIOGRAFÍA:

- Luis Ángel Dueñas Gómez, “Controles y Auditoria de los Sistemas de Información”, 2000, ORION EDITORES LTDA., Santafé de Bogotá.
- José Antonio Echenique,” Auditoria en Informática”, 1990, McGRAW-HILL, México.
- Dr. Wellington Ríos V. “Auditoria Informática”, 1994, EDI-ABACO Cia. Ltda., Ecuador
- Royal P. Fisher “Seguridad en los Sistemas Informáticos”, 1988, DÍAZ DE SANTOS, Madrid.
- Fernando Valencia”Sistemas de Información administración de las operaciones”, 1991, FES, Cali – Colombia.

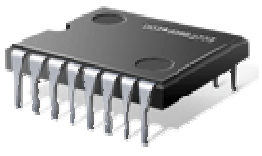
ANEXO 1.

RESUMEN DE INVENTARIO DE HARDWARE (SERVIDOR Y ESTACIÓN DE TRABAJO)

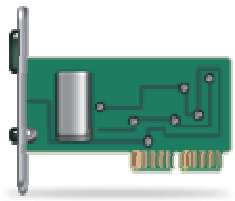
SERVIDOR

RESUMEN DE INVENTARIO DE HARDWARE CONTROLASISTENC

Descripción del sistema 	**Nombre:**	CONTROLASISTENC
	Fabricante:	
	Sistema operativo:	Windows XP Professional
	Paquete de servicio:	Service Pack 2
	Versión:	5.1.2600
	Usuario registrado:	dpsp
	Memoria física:	1024 Mb
	Dominio/ Grupo de trabajo:	SVRMATRIZ
	Modelo:	
	Número de serie:	55274-649-6478953-23578
	Organización:	dpsp
	Idioma del sistema:	Español (alfabetización internacional)
	Zona horaria del sistema:	(GMT -05:00) Hora est. del Pacífico de SA
	Usuario con sesión abierta:	Administrador
	Versión de Direct X:	9.0c
	Caja del sistema:	Unknown

Placa base 	**Procesador:**	Intel(R) Pentium(R) 4 CPU 2.80GHz
	Velocidad de reloj:	2800 MHz
	Fabricante del procesador:	Intel
	Etiqueta de	

	la BIOS:			
	Fabricante de la BIOS:	Intel Corp.		
	Versión de la BIOS:	VA84510A.86A.0030.P10.0402160229		
	Número de serie de la BIOS:			
	Fecha de instalación de la BIOS:	02/16/2004		
	Fabricante de la placa base:	Intel Corporation		
	Modelo de placa base:	D845GVSR		
	Versión de placa base:	AAC45441-302		
	Ranura de memoria 0:	J6G1	**Capacidad:**	1024 Mb
	Ranura de memoria 1:	J6G2	**Capacidad:**	0 Mb
	Ranura de sistema 0:	J7B2	**Disponibilidad:**	In use
	Ranura de sistema 1:	J8B1	**Disponibilidad:**	In use
	Ranura de sistema 2:	J9B1	**Disponibilidad:**	Available

Adaptador de red 	**Adaptador de red 1:**	Adaptador Fast Ethernet PCI CNet PRO200 - Minipuerto del administrador de paquetes
	Tipo de adaptador:	Ethernet
	Dirección IP:	10.64.32.224
	Subred IP:	255.255.240.0
	Gateway IP predeterminado:	10.64.32.51
	Servidor primario WINS:	0.0.0.0
	Servidor DNS:	200.105.225.2

	Servidor DHCP:	255.255.255.255
	Dirección MAC:	00-08-A1-60-46-F5

Adaptador de vídeo 	**Adaptador de vídeo 1:**	Intel(R) 82845G Graphics Controller
	RAM adaptador:	64 Mb
	Tipo DAC:	Internal
	Monitor de PC 1:	Monitor predeterminado
	Resolución de vídeo:	1280 x 720 x 32 bit
	Velocidad de regeneración:	60 Hz

Almacenamiento 	**Disco físico 1:**	ST380011A	
	Capacidad:	74.53 Gb	
	Disco lógico\Descripción\0:	C:	
	Sistema de archivos:	NTFS	
	Tamaño:	74.52 Gb	87% Libre

Varios 	**Teclado:**	Mejorado (clave 101 o clave 102)
	Tarjeta de sonido 1:	Realtek AC'97 Audio
	Dispositivo de comunicación 1:	SoftV92 Data Fax Modem
	Interfaz USB 1:	Intel(R) 82801DB/DBM USB Universal Host Controller - 24C2

	Interfaz USB 2:	Intel(R) 82801DB/DBM USB Universal Host Controller - 24C4
	Interfaz USB 3:	Intel(R) 82801DB/DBM USB Universal Host Controller - 24C7
	Interfaz USB 4:	Controladora de host universal mejorado 2.0 USB Intel (R) 82801DB/DBM - 24CD

Detalles de licencia de NetSupport ✔	**Cedido bajo licencia a:**	SISTEMAS
	Número de serie:	NSM309267
	Fecha de vencimiento:	Versión completa
	Clientes máximos:	1000

Impresoras 	**Impresora 1:**	Samsung ML-3560 Series PS
	Ubicación :	IP_10.64.32.49(0)
	Impresora 2:	Samsung ML-3560 Series PCL 6
	Ubicación :	IP_10.64.32.49(0)
	Impresora 3:	Samsung ML-3560 Series (Samsung 10.64.32.49)
	Ubicación :	IP_10.64.32.49(0)
	Impresora 4:	Samsung ML-3560 Series (Samsung 10.64.32.46)
	Ubicación :	IP_10.64.32.46(0)
	Impresora 5:	Samsung ML-3560 Series (Samsung 10.64.32.43)
	Ubicación :	IP_10.64.32.43(0)
	Impresora 6:	Samsung ML-3560 Series (Samsung 10.6.4.32.42)
	Ubicación :	IP_10.64.32.42(0)
	Impresora 7:	HP LaserJet P4010_P4510 Series PCL 6 (HP_COMTABILIDAD)
	Ubicación :	HPLaserJetP4014
	Impresora 8:	HP LaserJet P4010_P4510 Series PCL 6 (HP LJ P4010_P4510 FARMACIA)
	Ubicación :	HPLaserJetP4014_copy_1
	Impresora 9:	HP LaserJet P3005 PCL 6 (HP LJ 10.64.32.58)

	Ubicación :	HPLaserJetP3005_copy_3
	Impresora 10:	HP LaserJet P3005 PCL 6 (HP LJ 10.64.32.48)
	Ubicación :	HPLaserJetP3005_copy_1
	Impresora 11:	Samsung ML-3560 Series PCL 60
	Ubicación :	HPLaserJetP3005
	Impresora 12:	HP LaserJet P3005 PCL 6 (HP LJ 10.64.32.27)
	Ubicación :	IP_10.64.32.49(0)1
	Impresora 13:	HP LaserJet P3005 PCL 6 (HP LJ 10.64.32.230)
	Ubicación :	IP_10.64.32.49(0)2
	Impresora 14:	HP LaserJet P3005 PCL 6 (HP LJ 10.64.32.17)
	Ubicación :	IP_10.64.32.49(0)3
	Impresora 15:	HP LaserJet P3005 PCL 6 (HP LJ 10.64.32.131)
	Ubicación :	IP_10.64.32.49(0)4
	Impresora 16:	HP LaserJet P3005 PCL 6 (HP LJ 10.64.32.130)
	Ubicación :	IP_10.64.32.49(0)5
	Impresora 17:	HP LaserJet P3005 PCL 6 (\\Servidorapli00\HP LJ P3005 VSANITARIA)
	Ubicación :	IP_10.64.32.49(0)6

ANEXO 2.

RESUMEN DE INVENTARIO DE SOFTWARE (SERVIDOR Y ESTACIÓN DE TRABAJO)

RESUMEN DE INVENTARIO DE SOFTWARE CONTROLASISTENC

Resumen de inventario de
Software CONTROLASISTENC

Última modificación: 23 Sep 2009 11:57:07

Descripción	Empresa	Nombre de carpeta	Versión	Nombre de archivo
3D Pinball	Cinematronics	Pinball	5.1.2600.2180	PINBALL.EXE
7100A_C.Exe	WIZnet Corp.	LPSEG_Tool	3.00	7100A_C.exe
Address Book	Microsoft Corporation	Outlook Express	6.00.2900.2180	wab.exe
Aplicación MFC WORDPAD	Microsoft Corporation	Accesorios	5.1.2600.2180	wordpad.exe
Archivo de datos de Zone	Microsoft Corporation	Windows	1.2.626.1	shvlzm.exe
Archivo de datos de Zone	Microsoft Corporation	Windows	1.2.626.1	chkrzm.exe
Archivo de datos de Zone	Microsoft Corporation	Windows	1.2.626.1	Rvsezm.exe
Archivo de datos de Zone	Microsoft Corporation	Windows	1.2.626.1	bckgzm.exe
Archivo de datos de Zone	Microsoft Corporation	Windows	1.2.626.1	hrtzzm.exe
Asistente para la conexión a Internet	Microsoft Corporation	Connection Wizard	6.00.2900.2180	icwconn2.exe
Asistente para la conexión a Internet	Microsoft Corporation	Connection Wizard	6.00.2900.2180	inetwiz.exe
Asistente para la conexión a Internet	Microsoft Corporation	Connection Wizard	6.00.2900.2180	icwconn1.exe
Clip Organizer	Microsoft Corporation	Office12	12.0.4518.1014	MSTORE.EXE
HyperTerminal Applet	Hilgraeve, Inc.	Windows NT	5.1.2600.0	hypertrm.exe
Información del sistema	Microsoft Corporation	MSInfo	5.1.2600.0	msinfo32.exe
Intel(R) Application	Intel Corporation	Intel Application	Version 2.3.0.2160	intelata.exe

Accelerator		Accelerator		
Internet Explorer	Microsoft Corporation	Internet Explorer	6.00.2900.2180	IEXPLORE.EXE
Internet Signup	Microsoft Corporation	Connection Wizard	6.00.2600.0000	isignup.exe
LogMeIn Desktop Application	LogMeIn, Inc.	x86	4.0.966	LogMeInToolkit.exe
Microsoft (R) Address Book Import Tool	Microsoft Corporation	Outlook Express	6.00.2900.2180	wabmig.exe
Microsoft Office Access	Microsoft Corporation	Office12	12.0.4518.1014	MSACCESS.EXE
Microsoft Office Diagnostics	Microsoft Corporation	OFFICE12	12.0.4518.1014	OFFDIAG.EXE
Microsoft Office Excel	Microsoft Corporation	Office12	12.0.4518.1014	EXCEL.EXE
Microsoft Office Groove	Microsoft Corporation	Office12	4.2.0.2623	GROOVE.EXE
Microsoft Office InfoPath 2007	Microsoft Corporation	Office12	12.0.4518.1014	INFOPATH.EXE
Microsoft Office OneNote	Microsoft Corporation	Office12	12.0.4518.1014	ONENOTE.EXE
Microsoft Office Outlook	Microsoft Corporation	Office12	12.0.4518.1014	OUTLOOK.EXE
Microsoft Office Picture Manager	Microsoft Corporation	Office12	12.0.4518.1014	OIS.EXE
Microsoft Office PowerPoint	Microsoft Corporation	Office12	12.0.4518.1014	POWERPNT.EXE
Microsoft Office Publisher	Microsoft Corporation	Office12	12.0.4518.1014	MSPUB.EXE
Microsoft Office Word	Microsoft Corporation	Office12	12.0.4518.1014	WINWORD.EXE
Outlook Express	Microsoft Corporation	Outlook Express	6.00.2900.2180	msimn.exe

PROSet Module	Intel(R) Corporation	PROSet	6.2.35.0	PROSet.exe
Reproductor de Windows Media	Microsoft Corporation	Windows Media Player	9.00.00.3250	wmplayer.exe
RtlRack MFC Application	Realtek Semiconductor Corp.	AvRack	1.6.0.0	rtlrack.exe
Visor de conferencia de transmisión múltiple del marcador e IP TAPI 3.0	Microsoft Corporation	Windows NT	5.1.2600.2180	dialer.exe
Win32 Cabinet Self-Extractor	Microsoft Corporation	Install	5.50.4134.600	msnsusii.exe
Windows Media Player	Microsoft Corporation	Windows Media Player	6.4.09.1125	mplayer2.exe
Windows Messenger	Microsoft Corporation	Messenger	Version 4.7.3000	msmsgs.exe
Windows Movie Maker	Microsoft Corporation	Movie Maker	2.1.4026.0	moviemk.exe
Windows® NetMeeting®	Microsoft Corporation	NetMeeting	3.01	conf.exe
XML Editor	Microsoft Corporation	OFFICE12	12.0.4518.1014	MSOXMLED.EXE

ANEXO 3.

POLÍTICAS PARA EL USO DE LOS COMPUTADORES DE LA DPSP

MINISTERIO DE SALUD PÚBLICA
DIRECCIÓN PROVINCIAL DE SALUD DE PICHINCHA
GESTIÓN INFORMÁTICA

POLÍTICAS PARA EL USO DE LOS COMPUTADORES DE LA DIRECCIÓN PROVINCIAL DE SALUD DE PICHINCHA

La seguridad informática es la disciplina orientada a definir y establecer mecanismos de resguardo y protección permanente de la información, por lo cual es necesario cumplir ciertas normas.

1. El computador y periféricos asignados a cada usuario, están bajo su responsabilidad; por lo tanto el usuario deberá responder por pérdida, cambio de componentes o uso indebido de los mismos.
2. No se permite fumar, comer o beber mientras se está usando un PC.
3. Se encuentra totalmente prohibido colocar aparatos magnéticos cerca de los computadores.
4. Todo equipo deberá estar conectado a su respectivo regulador de voltaje.
5. No se debe permitir que personas ajenas a la Institución hagan uso de los ordenadores, ni copien en dispositivos como CD, diskette, flash, la información de los mismos**.**
6. Al culminar la jornada de trabajo los equipos deberán ser apagados adecuadamente por la opción *Apagar Sistema*, la misma que es proporcionada por el sistema operativo del computador y deberán ser cubiertos con sus respectivos cobertores si los tuviese**.**
7. Se encuentra terminantemente prohibido mover o reubicar los equipos o periféricos de un proceso a otro, sin previa notificación y autorización de Proceso de Gestión Informática.
8. En caso de existir reubicación de algún usuario a otro equipo, éste deberá ser notificado al Proceso de Gestión Informática para su registro.
9. Los equipos no deben ser abiertos por ningún funcionario que no pertenezca al Proceso de Gestión Informática.

10. Está terminantemente prohibido agitar el tonner en las impresoras láser, cuando la calidad de la impresión es deficiente.
11. Está prohibido conectar otro tipo de aparatos eléctricos en la toma destinada para computadores.
12. Se encuentra terminantemente prohibido el ingreso a la DPSP de equipos de computación que no pertenezcan a la institución.
13. Los usuarios deberán crear una carpeta específica con su información, ya que en caso de reparación de algún equipo, Gestión Informática respaldará únicamente está carpeta.
14. No divulgar información confidencial a personas no autorizadas**.**
15. No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que o estén directamente relacionadas con el trabajo.
16. Proteger meticulosamente su contraseña de usuario y evitar que sea vista por otros en forma inadvertida, para la seguridad de la información.
17. Debe activar el protector de pantalla manualmente cada vez que se ausente de su oficina**.**
18. Está terminantemente prohibida la instalación y modificación de la configuración tanto del software como del hardware así como también el uso de software de distribución gratuita shareware (juegos o programas), a menos que haya sido previamente aprobado por el Proceso de Gestión Informática.
19. El usuario del equipo debe poseer como máximo el 3% de la capacidad de almacenamiento en el disco duro de su CPU para archivos de audio, video e imagen.
20. Reportar inmediatamente a su jefe inmediato o a un funcionario del Proceso de Gestión Informática cualquier evento que pueda comprometer la seguridad de la DPSP y a sus recursos informáticos, como el contagio de virus, intrusos que ocasionarán modificación o pérdida de datos y otras actividades**.**
21. Los programas (software) adicionales que se encuentren instalados y no sean herramientas utilizadas en la DPSP, serán eliminados.

22. A menos que se indique lo contrario, los usuarios deben asumir que todo el software de la DPSP está protegido por derechos de autor y requiere licencia de uso.

23. Debe respetarse y no modificar la configuración de hardware y software establecida por el Proceso de Gestión Informática**.**

24. Cualquier falla en la red debe reportarse inmediatamente al personal del Proceso de Gestión Informática ya que podría causar problemas serios como pérdida de la información o disponibilidad de los servicios.

25. No deben usarse disket u otros medios de almacenamiento en cualquier computadora de la DPSP a menos que hayan sido previamente verificados que están libres de virus u otros agentes dañinos**.**

26. Los usuarios de PCs son responsables de proteger los programas y datos contra pérdida o daño**.**

27. El uso del internet será monitoreado constantemente y su mala utilización será objeto de suspensión del servicio sin previo aviso.

28. Al recibir correos con archivos adjuntos verificar por medio de un antivirus antes de abrirlos para que su máquina no se infecte de virus.

29. Antes de abrir un archivo del internet verificar que no esté contaminado con virus.

30. No abrir muchas ventanas de internet porque entorpece al computador y se hace más lenta.

31. Al enviar un archivo adjunto primero verificar que esté libre de virus para prevenir el ingreso de intrusos a la red.

32. Para el envió de mensajes y documentación debe utilizarse Outlook Express. Para que la información llegue únicamente a la persona enviada.

33. El correo electrónico de la DPSP será únicamente para asuntos laborales.

34. No enviar correos con muchos archivos adjuntos puesto que esto puede ocasionar una pérdida de información o provocar una demora en el envío.

35. Los mensajes que ya no se necesitan deben ser eliminados semanalmente de su área de almacenamiento. Con esto se reducen los

riesgos de que otros puedan acceder a esa información y además se libera espacio en la ***bandeja de entrada***.

36. La solicitud de una nueva cuenta o el cambio de privilegios debe ser hecha por escrito y debe ser debidamente aprobada por el Proceso de Gestión Informática.

37. Evitar los correos en cadenas ya que es causante de que los archivos contengan virus.

38. Nunca debe compartirse la contraseña del correo electrónico o revelarla a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.

39. El Proceso de Gestión Informática, realizará revisiones del contenido de información sin previo aviso a los usuarios. En caso de que se hayan incumplido las normas anteriormente mencionadas; el usuario será notificado para fines pertinentes por la autoridad.

40. Es política de La DPSP monitorear regularmente las comunicaciones. Sin embargo, el uso y el contenido de las comunicaciones puede ocasionalmente ser supervisado en caso de ser necesario para actividades de mantenimiento, seguridad o auditoría. Puede ocurrir que el personal técnico vea el contenido de un mensaje de un empleado individual durante el curso de resolución de un problema.

41. El usuario no puede compartir carpetas por más de dos días.

Dr. Luis Fernando Calderón

Director Provincial de Salud de Pichincha

ANEXO 4.

EVALUACIÓN DE LA SEGURIDAD

SEGURIDAD FÍSICA

CENTRO DE CÓMPUTO

1. ¿Está el Centro de Cómputo en un lugar de alto tráfico de personas?
   Si No√
2. ¿Se tiene materiales o paredes inflamables dentro del centro de cómputo?
   Si√
   No
3. ¿Se tiene paredes que despiden polvo? Si√ No
4. ¿Existe lugar suficiente para los equipos? Si No√
5. ¿Está sobresaturada la instalación? Si√ No
6. ¿Se tiene lugar previsto para?:
   - **a.** Almacenamiento de equipos magnéticos. Si No√
   - **b.** Formatos y papel para impresora. Si No√
   - **c.** Mesas de trabajo y muebles. Si No√
   - **d.** Área para mantenimiento de computadores. Si No√
   - **e.** Equipos de telecomunicaciones Si No√
   - **f.** Área de programación Si No√
   - **g.** Consolas del operador Si No√
   - **h.** Área de recepción de los equipos Si No√
   - **i.** Microcomputadoras Si No√
   - **j.** Fuentes de poder Si No√
   - **k.** Bóveda de seguridad(antiincendio) Si No√
7. ¿Se tiene piso falso? Si No√

   En caso afirmativo
   - **a.** ¿Está limpia la cámara plena? Si No
   - **b.** ¿Es de fácil limpieza? Si No
   - **c.** ¿El piso es antiestático? Si No

AIRE ACONDICIONADO

1. ¿La temperatura en la que trabajan los equipos es la recomendada por el proveedor? Si
   No√
2. ¿Los ductos del aire acondicionado cuentan con alarmas contra intrusos? Si
   No√
3. ¿Se controla la humedad de acuerdo con las especificaciones del proveedor? Si No√
4. En caso de afirmativo:
   a. ¿De qué forma?

   ---

   b. ¿Con qué periodicidad?

INSTALACIÓN ELÉCTRICA Y SUMINISTRO DE ENERGÍA

1. ¿Se cuenta con tierra física? Si√ No
2. ¿La tierra física cumple con las disposiciones del proveedor de equipos de cómputo? Si√
   No
3. ¿El cableado se encuentra debidamente instalado? Si No√
4. ¿Los cables se encuentran debidamente identificados (positivo, negativo, tierra)? Si
   No√
5. ¿En los contactos, está identificado el positivo, negativo y tierra física? Si No√
6. ¿Se cuenta con planos de instalación eléctrica actualizados? Si No√
7. ¿Se tiene conectado a los contactos de equipo de cómputo otro equipo electrónico? Si√ No

8. ¿Se tiene instalación eléctrica de equipo de cómputo independiente de otras instalaciones eléctricas? Si√ No

9. ¿Se utiliza material antiestático? Si√ No

10. ¿Se tiene reguladores para los equipos de cómputo? Si√ No

11. ¿Se tiene equipo ininterrumpible? Si√ No

12. ¿Dura el tiempo suficiente para respaldar los archivos o para continuar el proceso? Si√ No

13. ¿Se tiene generadores de corriente ininterrumpida? Si No√

En caso afirmativo:

a. ¿De qué tipo?

_____

b. ¿Se prueba su funcionamiento? Si No

c. ¿Con qué periodicidad?

_____

En caso negativo:

¿Por qué?

_____

14. ¿Se tiene switch de apagado en caso de emergencia en lugar visible? Si√ No

15. ¿Los cables están dentro de paneles y canales eléctricos? Si√ No

16. ¿Existen tableros de distribución eléctrica? Si√ No

SEGURIDAD DE AUTORIZACIÓN DE ACCESOS

1. ¿Se han adoptado medidas de seguridad en PGI? Si√ No

2. ¿Existe una persona responsable de la seguridad? Si No√

3. ¿Se controla el trabajo fuera de horario? Si No√

4. ¿Se registran las acciones de los operadores para evitar que realicen alguna que pueda dañar el sistema? Si No√

5. ¿Se identifica a la persona que ingresa? Si No√

6. En caso afirmativo:

a. ¿De qué forma?

---

7. ¿Cómo se controla el acceso?:

a. Vigilante ()

b. Recepcionista ()

c. Tarjeta de control de acceso (√)

d. Puerta de combinación ()

e. Puerta con cerradura ()

f. Puerta electrónica ()

g. Puertas dobles ()

h. Registro de entradas ()

i. Escolta controlada ()

j. Alarmas ()

k. Tarjetas magnéticas ()

l. Control biométrico ()

m. Identificación personal ()

8. ¿Existe vigilancia en el área de servidores las 24 horas? Si No√

9. ¿Se han instruido a estas personas sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización? Si No√

10. ¿Son controladas las visitas y demostraciones en el centro de cómputo? Si No√

En caso afirmativo:

¿Cómo son controladas?

---

11. ¿Se registra el acceso cuando personas ajenas al PGI ingresan? Si No√

DETECCIÓN DE HUMO Y FUEGO. EXINTORES

1. ¿Existe alarma para:
    a. Detectar fuego (calor o humo)en forma automática? ()
    b. Avisar en forma manual la presencia del fuego()
    c. Detectar una fuga de agua ()
    d. Detectar magnetos (√)
    e. No existe? ()
2. ¿Estas alarmas están:
    a. En el área de servidores? ()
    b. En la cintoteca y discoteca? ()
    c. En las bodegas? ()
    d. En otros lados ()
3. ¿Existe alarma para detectar condiciones anormales del ambiente:
    a. En el área de servidores? ()
    b. En la cintoteca y discoteca? ()
    c. En las bodegas? ()
    d. En otros lados ()
    e. ¿Cuáles?

---

4. ¿La alarma es perfectamente audible? Si No√
5. ¿La alarma esta conectada:
    a. Al puesto de guardias? ()
    b. A la estación de bomberos? ()
    c. A otro lado? ()
    d. Otros ()
6. ¿Existen extintores de fuego?
    a. Manuales (√)
    b. Automáticos ()
    c. No existen ()
7. ¿Se ha adiestrado el personal en el manejo de los extintores?
    Si No√
8. Los extintores, manuales o automáticos, funcionan a base de:
    a. Agua ()
    b. Gas (√)

c. Otros ()

9. ¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores? Si No√

10. ¿Conoce usted, cual es el número de extintores que hay en la institución y su estado? Si

No√

11. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?

Si No√

12. ¿Sabe el personal del PGI que hacer en caso de que ocurra una emergencia en el cuarto de servidores ocasionada por fuego?

Si No√

13. ¿El personal ajeno al PGI sabe qué hacer en el caso de una emergencia (incendio)? Si√ No

14. ¿Existe salida de emergencia? Si No√

15. ¿Se tiene identificadas y señaladas las salidas de emergencia?

Si No√

16. ¿Se encuentran las señalizaciones en la parte superior de los pasillos?

Si No√

17. ¿Existe un plan de emergencia en la Institución que abarque estas eventualidades y demás? Si No√

18. ¿Se tiene bóveda contra incendio? Si No√

19. ¿Se han tomado medidas para minimizar la posibilidad de fuego:

a. Evitando artículos inflamables en el PGI? ()

b. Evitando artículos inflamables en el área de servidores?

c. Prohibiendo fumar? ()

d. Vigilando y manteniendo el sistema eléctrico? ()

e. No se ha previsto (√)

SEGURIDAD EN GENERAL

1. ¿Se controla el préstamo de:

a. Elementos magnéticos? ()

b. Equipos? (√)

c. Software? ()

2. Explique la forma en que se ha clasificado la información: vital, esencial, no esencial, etcétera.

No existe clasificación de la información

---

3. Describa que Sistemas son considerados sensibles o críticos

Sistema de control Sanitario, Sistema de Farmacia, y el Sistema de Estadísticas

---

---

4. ¿Se cuenta con copias de los archivos de sistemas en un lugar distinto al de los computadores? Si No√

5. ¿Explique la forma en que están protegidas físicamente estas copias para garantizar su integridad en caso de incendio, inundación, terremoto, etcétera:

- **a.** Bóveda ()
- **b.** Cajas de seguridad ()
- **c.** Otros ()

No existe protección

---

6. ¿Se tienen establecidos procedimientos de actualización para estas copias? Si No√

7. Indique el número de copias que se tienen, de acuerdo con la forma en que se clasifica la información.

No existe dicho registro de clasificación

---

8. ¿Existe departamento de auditoría interna en la institución?

Si No√

9. ¿Este departamento de auditoria interna conoce todos los aspectos de los sistemas? Si

No√

10. ¿Cuándo se efectúan modificaciones a los programas, a iniciativa de quién?:

- **a.** Usuario ()

b. Director de la DPSP ()

c. Coordinador del PGI ()

d. Programador. ()

e. Otras(especifique) (√)

Disposición del Coordinador del Departamento

---

11. La solicitud de modificaciones a los programas se hacen en forma:

a. Oral ()

b. Escrita (√)

*En caso de escrita solicitar formato

12. ¿Existe control estricto en las modificaciones? Si√ No

En caso afirmativo:

a. Se revisa que tengan la fecha de las modificaciones cuando se hayan efectuado? Si No√

13. Se verifica identificación:

a. De la Terminal? ()

b. Del usuario? ()

c. No se pide identificación (√)

14. ¿Se ha establecido el nivel de usuario de la información?

Si√ No

15. ¿Se ha establecido un número máximo de violaciones en sucesión para que la computadora cierre esa Terminal y se de aviso al responsable de ella? Si No√

16. ¿Se registra cada violación a los procedimientos con el fin de llevar estadísticas y frenar las tendencias mayores? Si No√

17. ¿Existen controles y medidas de seguridad sobre las siguientes operaciones? Si No

¿Cuáles son?

a. Recepción de documentos ()

b. Información confidencial ()

c. Captación de documentos ()

d. Cómputo electrónico ()

e. Programas ()

f. Discotecas ()

g. Documentos de salida ()

h. Archivos magnéticos ()

i. Operaciones del equipo de computación ()

j. Seguros contra robo e incendio ()

k. Otras(especifique) ()

No existe

REDES Y COMUNICACIÓN

1. ¿Cuántos tipos de red existen y cuáles son:?

Dos tipos, Inalámbrica y Alámbrica

---

2. ¿Qué topología utilizan?

a. Estrella √

b. Malla

c. Bus

3. ¿Qué tecnología utilizan?

Tecnología TCP/IP

---

4. ¿Cuál es el tipo de conexión a líneas públicas?

a. Interna PBX (√)

b. Compartida PBX ()

c. Línea Directa ()

d. No Aplica ()

e. Otro ()

---

5. ¿Qué protocolos son usados?

a. X25 ()

b. SDLC/HDLC ()

c. LAN/ETHERNET/TCPIP (√)

d. Otro ()

---

6. ¿Cuántos usuarios tienen acceso al sistema GESTOR (ERP)?

- **a.** Menos de 50 (√)
- **b.** Entre 50-100 ()
- **c.** Más de 100 ()

7. ¿Cuántos usuarios tienen acceso al sistema VGSIPF?

- **a.** Menos de 50 ()
- **b.** Entre 50-100 (√)
- **c.** Más de 100 ()

8. ¿Cuántos usuarios tienen acceso al sistema SISPROD?

- **a.** Menos de 50 (√)
- **b.** Entre 50-100 ()
- **c.** Más de 100 ()

9. ¿Cuántos usuarios tienen acceso al sistema SGM?

- **a.** Menos de 50 (√)
- **b.** Entre 50-100 ()
- **c.** Más de 100 ()

10. ¿Cuántos usuarios tienen acceso al sistema ANGEL?

- **a.** Menos de 50 (√)
- **b.** Entre 50-100 ()
- **c.** Más de 100 ()

11. ¿Cuántos usuarios tienen acceso al sistema SIGEF?

- **a.** Menos de 50 (√)
- **b.** Entre 50-100 ()
- **c.** Más de 100 ()

12. ¿Cuántos usuarios tienen acceso al sistema CONTROL DE CORRESPONDENCIA?

- **a.** Menos de 50 (√)
- **b.** Entre 50-100 ()
- **c.** Más de 100 ()

13. ¿Cuántos usuarios tienen acceso al sistema TRANSPORTES?

- **a.** Menos de 50 (√)
- **b.** Entre 50-100 ()
- **c.** Más de 100 ()

14. ¿Han sido definidos los requerimientos mínimos en términos de disponibilidad y rendimiento?

Si No√

15. ¿Qué facilidades de recuperación de la red existe en el lugar?

a. Líneas de reserva/adicional ()

b. Rutas alternadas ()

c. Ninguna de estas (√)

16. ¿Existe una transmisión de datos sensitiva o confidencial?

Si No√

17. ¿Cuál es el porcentaje de tiempo fuera que ha tenido la institución debido a fallas en la red de comunicaciones en los últimos 12 meses?

a. Menor del 1% ()

b. Mayor del 1% (√)

18. ¿Se encriptan los datos de transmisión? Si No√

19. ¿Cuál es el principal medio de transmisión usado?

a. Cobre/Par Trenzado (√)

b. Coaxial Cable ()

c. Satélite/Microondas ()

d. Fibra Óptica ()

20. ¿El cableado de comunicaciones de que categoría es:?

a. Categoría 5 ()

b. Categoría 5e (√)

c. Categoría 6 ()

d. Categoría 6a ()

e. Otro ()

---

21. ¿El nivel de tráfico es monitoreado? Si No√

22. ¿Las asignaciones y reasignaciones de puerto se registran y documentan?

Si No√

23. ¿Qué tan frecuente se reasignan puertos?

No se realiza

24. ¿Existen sistemas de comunicación alternativos en caso de avería o fallo? Si No√

25. En los contratos de comunicaciones ¿están claramente reflejados los parámetros que definen la calidad de servicio, como ancho de banda, tiempo de respuesta de averías.?

Si No√

26. ¿Existe algún plano de la instalación del cableado y sistemas de comunicaciones en el edificio? Si√ No

27. ¿Se realizan pruebas periódicas para garantizar la calidad de las líneas y sistemas de comunicación? Si No√

28. El cableado de comunicaciones ¿Es fácilmente accesible para las labores de mantenimiento?

Si No√

29. El personal de mantenimiento ¿Es custodiado mientras realizan sus labores? Si No√

30. ¿Los equipos de comunicaciones se encuentran en un lugar de acceso restringido? Si No√

31. ¿El cableado de comunicaciones está separado de la instalación eléctrica? Si

No√

32. ¿Existe alguna protección física para los principales cables de conexión con el proveedor de comunicaciones? Si No√

PROCESOS EN LÍNEA

1. ¿El personal del proceso de Informática está informado de los procesos que los usuarios realizan en línea (procesos bancarios, transacciones, o transferencias? Si No√

2. ¿Qué procesos son?

No, el Departamento del PGI sabe de la existencia, pero no conoce sus procesos.

3. ¿Qué Proceso lo ejecuta?

El Subproceso de Tesorería

---

4. ¿Con qué frecuencia?

Mensual

---

5. ¿Qué protección existe para este tipo de transacciones?

Ninguna

ANEXO 5.

EVALUACIÓN DE CONTROL INTERNO

Cliente: Dirección Provincial de Salud de Pichincha (DPSP)				
Fecha:				
Departamento/Proceso: Área de Seguridad Física				
Objetivo: Evaluar la Seguridad Física del Proceso de Gestión Informática				
Título: Cuestionario Interno				
Pregunta	**Si**	**No**	**N/C**	**Observación**
¿Existen procedimiento de control de accesos?	√			Tarjetas Magnéticas
¿Existe una política de seguridad física en la Institución y en el PGI?			√	
¿Existe un plan de emergencia en la Institución y en el PGI?		√		
¿Se cuenta con algún control de acceso?	√			Tarjetas Magnéticas
¿Este control abarca el Área de Servidores?		√		
¿Se registra al personal de la institución o visitante que ingresa al PGI?		√		
¿Se conoce el motivo por el cual necesita estar en el PGI?		√		
¿Se escolta al personal o visitante durante el tiempo que este en el PGI?		√		
¿Se registra las actividades realizadas por el visitante?		√		
Una vez terminada la visita se revisa ¿bolsos, mochilas, etc.?	√			Fuera del Edificio
¿El área de servidores tiene algún control de acceso?		√		
¿Cualquier persona puede ingresar al área de servidores?	√			
Todo el personal del PGI ¿tiene autorización para ingresar al área de servidores?	√			

¿Tiene él personal del PGI un listado con los números de teléfono más importantes en caso de emergencia?	√			
¿Se evalúa el estado físico del hardware, periférico, y equipos asociados?		√		
¿Se evalúa el uso y rendimiento del sistema computacional y sus periféricos asociados?		√		
¿Existen rutinas internas para el correcto funcionamiento de los servidores y dispositivos de comunicaciones?		√		
Responsables: Egr. Sonia Buñay & Egr. Emilly Guanotuña				
N/C: No conoce.				

Cliente: Dirección Provincial de Salud de Pichincha (DPSP)				
Fecha:				
Departamento/Proceso: Área de Seguridad Lógica				
Objetivo: Evaluar la Seguridad Lógica en el Proceso de Gestión Informática				
Título: Cuestionario Interno				
Pregunta	**Si**	**No**	**N/C**	**Observación**
¿Existen procedimiento de control de accesos lógico?	√			Existe Autentificación de usuarios en la red
El personal del PGI ¿está en capacidad de resolver problemas que se generen por permisos, contraseñas incorrectas accesos denegados a BDD, etc.?		√		
¿Existe control en la administración de contraseñas, con que periodicidad?		√		
¿Qué tipo de controles existen para evitar Software`s Maliciosos?				Antivirus
¿Existen controles de uso de		√		

contraseñas de Administrador?				
¿Existe administración y control de IP's?		√		
¿Existe control de versiones en los sistemas implementados?		√		
¿Existe control y registro de errores que se generan en los sistemas implementados y/o Sistemas Operativos?		√		
¿Se evalúa el rendimiento y el uso de los sistemas implementados?		√		
¿Existe control en la protección y periodicidad de los respaldos de bases de datos, software e información importante de la organización?		√		
¿Se evalúa la seguridad en el procesamiento de la información?		√		
¿Que procedimiento de cifrados utilizan?			√	
¿Se comparte información mediante la red?	√			
¿Existen controles en el correo electrónico?		√		
¿Existe control en modificación, actualización y administración de la página web?		√		
¿Existe un control de licencias de software?		√		
¿Existe protección contra los actos ilegales en contra de los sistemas, activos informáticos e información?		√		
¿Se evalúa la configuración del equipo de cómputo?		√		
¿Existen rutinas internas para el correcto funcionamiento de las aplicaciones?		√		

Responsables: Egr. Sonia Buñay & Egr. Emilly Guanotuña
N/C: No conoce.

ANEXO 6.

HALLAZGOS ENCONTRADOS Y

FORMULARIO DE VISITAS

FORMULARIO DE VISITAS
Descripción: Rack de Telecomunicaciones
Área: FARMACIA - DPSP
Fecha: 02 - Junio - 2009
Observaciones
El Rack de Telecomunicaciones se encuentra al alcance de cualquier usuario, y con UPS obsoleto que no cumple su función.
Responsables:
Egr. Sonia Buñay – Egr. Emilly Guanotuña

HALLAZGOS DE AUDITORÍA	
TÍTULO: Rack de Telecomunicaciones	
1. **Condición:** El Rack no cuenta con medidas de seguridad (se encuentra ubicado cerca del baño y debajo de la tubería de agua), el UPS no cumple su función, no existe etiquetación en los patch cord ni en los dispositivos de red	
2. **Criterio:** En la instalación de este rack no fue realizado un estudio de acuerdo a estándares de cableado ***ANSI/TIA/EIA-569-B***	
3. **Causa:** Mal distribución de los espacios	
4. **Riesgo**: Daño de los equipos, Ruptura de tuberías, Pérdidas de Productividad de Farmacia	
5. **Observación:** El nivel de riesgo es Bajo	
6. **Recomendación:** Sugerimos se reubique o se cambie el Rack por un armario cerrado y sobre todo que se cambie de UPS.	
Responsables:	**Se informa a:**
Egr. Sonia Buñay – Egr. Emilly Guanotuña	**Ing. Maritza Badillo**

FORMULARIO DE VISITAS

Descripción: Cableado de red antiguo
Área: FARMACIA - DPSP
Fecha: 02 - Junio - 2009
Observaciones
El cableado de Red anterior no ha sido retirado provocando confusiones en la conexión y mal aspecto por su deterioro.
Responsables:
Egr. Sonia Buñay – Egr. Emilly Guanotuña

HALLAZGOS DE AUDITORÍA	
TÍTULO: Cableado de red antiguo	
1. Condición: La red ha sido cambiada hace más de cinco años, pero el cableado anterior no ha sido removido.	
2. **Criterio:** No cumpliendo con la norma ***ISO/IEC 14763-2 Prácticas de Planificación e Instalación***	
3. Causa: Falta de organización en los trabajos ejecutados por parte del Proceso de Gestión Informática	
4. Riesgo: Confusión por parte de los usuarios al momento de conectar los equipos a la red, provocando así perdida de tiempo y que los usuarios no tengan los recursos de la red necesarios.	
5. Observación: El nivel de riesgo es Bajo	
6. Recomendación: Sugerimos cumplan con las normas expuestas.	
Responsables:	**Se informa a:**
Egr. Sonia Buñay – Egr. Emilly Guanotuña	**Ing. Maritza Badillo**

HALLAZGOS DE AUDITORÍA

TÍTULO: Sistemas Informáticos instalados sin informar al PGI	
1. **Condición:** El sistema Megan(Sistema de activos fijos y control de descargo de mercadería) ha sido instalado al igual que su Base de Datos en un equipo del Proceso de Servicios Institucionales sin ninguna autorización del PGI, y este sistema manifiesta problemas ya que el equipo se desconecta contantemente de la red provocando inoperatividad.	
2. **Criterio:** Esta decisión de instalación del sistema no fue acertada ya que un sistema de este tipo de información tan sensible se debió instalar en un servidor y bajo las normas de resguardo de backup de la información	
3. **Causa:** Poco protagonismo del PGI en la institución y falta de un inventario de Software´s y herramientas informáticas.	
4. **Riesgo:** Perdida de información e inoperatividad	
5. **Observación:** El nivel del riesgo es Alto	
6. **Recomendación:** Ya que el riesgo es alto se recomienda trasladar la Base de Datos y el sistema a un servidor y exigir a la empresa proveedora del software una capacitación técnica del sistema, manuales y demás elementos que permita al PGI dar un correcto soporte a los usuarios acerca de este sistema.	
Responsables:	**Se informa a:**
Egr. Sonia Buñay – Egr. Emilly Guanotuña	**Ing. Maritza Badillo**

HALLAZGOS DE AUDITORÍA
TÍTULO: Desconexión de la red de la mayoría de equipos
1. **Condición:** Los equipos de los diferentes procesos que existen en la institución, tienen constantes perdidas de la señal inalámbrica causando el impedimento al momento de imprimir y al usar el internet.
2. **Criterio:** Para este tipo de inconveniente se debe considerar la propagación de virus en la red, desactualización del antivirus o el simple

hecho de no contar con uno, pone en riesgo a los equipos y por esta razón los virus bajan los servicios de red, y además el material de los que están construidas las oficinas ya que son mixtas se debe considerar la inclusión de otro Access Point o de equipos repetidores de señal, ya que estas obstruyen la señal.	
3. **Causa:** Existen equipos sin antivirus o antivirus desactualizados No se realizó un análisis para la implementación de la red inalámbrica, ya que los Access Points esta situados en lugares poco estratégicos provocando que la señal no se propague de manera regular.	
4. **Riesgo:** Inoperatividad, usuarios y equipos sin recursos de red.	
5. **Observación:** El nivel del riesgo es Alto	
6. **Recomendación:** Adquirir un nuevo antivirus o el que existe contratar mas licencias, reubicar los Access Points y adquirir nuevos para ubicar en lugares que no llegan la señal, como también para el caso en que uno de ellos tuviera un desperfecto y no dejar inoperativo algún departamento.	
Responsables:	**Se informa a:**
Egr. Sonia Buñay – Egr. Emilly Guanotuña	**Ing. Maritza Badillo**

HALLAZGOS DE AUDITORÍA
TÍTULO: No existe un control en el análisis para la asignación de un equipo de cómputo a los usuarios.
1. **Condición:** El PGI no realiza un debido análisis del equipo a asignar a los usuarios, no toman en cuenta si este se ajustará a las necesidades operativas del usuario según sus funciones, llegando a asignar computadores con características actuales a usuarios que tan solo realizan oficios, mientras otros usuarios que trabajan diariamente en sistemas y herramientas informáticas que necesitan más recursos del computador teniendo ellos equipos obsoletos(Pentium I, II, III), por otro lado el Proceso de Recursos Humanos no informa de la existencia de nuevo personal contratado y sus funciones que realizará dentro de la

institución generando la asignación de computadores de manera acelerada y sin estudio.	
2. **Criterio:** No existe un análisis previo de equipos ya que estos no están reflejados en ningún manual de procedimientos.	
3. **Causa:** Falta de Procedimientos por la Coordinación	
4. **Riesgo:** Afectación en la Productividad	
5. **Observación:** El nivel de riego es Bajo	
6. **Recomendación:** 7. Coordinar con el Proceso de Recursos Humanos y definir controles al momento de ingreso y egresos de personal de la Institución, ya que el PGI debe velar por la seguridad de la información de la Institución, además debe analizar según los roles a cumplir de cada empleado para la entrega de su equipo de cómputo.	
Responsables:	**Se informa a:**
Egr. Sonia Buñay – Egr. Emilly Guanotuña	**Ing. Maritza Badillo**

HALLAZGOS DE AUDITORÍA
TÍTULO: El Proceso de Gestión Informática no cuenta con un Plan de Contingencia, Plan Estratégico, Plan Orgánico Funcional, Plan Orgánico Estructural, Manual de Normas, Manual de Procedimientos.
1. **Condición:** El PGI no cuenta con documentos e instructivos que le ayuden a guiar mediante normas preestablecidas a sus procesos, estando este departamento hiendo a la deriva.
2. **Criterio:** La coordinación de este departamento ya sea anterior o actual no ejecuta un enfoque del rumbo y los objetivos que debe tener el PGI, ya que no generan normas, instructivos, procedimientos que garanticen un buen desarrollo de las actividades.
3. **Causa:** Poco compromiso en precautelar la seguridad lógica y física de los recursos informáticos en la institución
4. **Riesgo:** Desequilibrio en la seguridad de todos los ámbitos a nivel informático.

5. **Observación:** El nivel de riego es Alto

6. **Recomendación:**

La coordinación del PGI debe realizar:

Un Plan de Contingencia (P.C) que garantice la reanudación de las operaciones en corto tiempo después de un desastre, este debe ser actualizado con frecuencia, especificar que procesos va a cubrir el P.C, su idoneidad, pruebas para l reanudación, etc.

Plan Estratégico que defina las actividades y procesos a cumplir dentro de este departamento.

Plan Orgánico Funcional debe especificar los cargos, responsables y funciones que cada técnico del PGI posee de acuerdo a su perfil profesional.

Plan Orgánico Estructural debe definir y notificar a los técnicos la estructura orgánica que tiene el PGI.

Manual de Procedimientos que indique los procesos que se deben realizar dentro del PGI basados en normas.

Responsables:	**Se informa a:**
Egr. Sonia Buñay – Egr. Emilly Guanotuña	**Ing. Maritza Badillo**

HALLAZGOS DE AUDITORÍA

TÍTULO: No existe normas de respaldos de la información de los usuarios

1. **Condición:** Los técnicos realizan el formateo de los equipos si obtener respaldos previamente, ocasionando malestar en los usuarios y pérdida de posible información importante para la institución.
2. **Criterio:** No existe un plan de procedimientos para este tipo de actividades.
3. **Causa**: Poco compromiso en precautelar la seguridad de la información.
4. **Riesgo:** Perdida de productividad e información importante y necesaria para la institución y usuario.
5. **Observación:** El nivel de riesgo es Alto
6. **Recomendación:**

Mantener rígidas normas de obtención de respaldos de la información de

los equipos previo a su respectivo formateo.	
Responsables:	**Se informa a:**
Egr. Sonia Buñay – Egr. Emilly Guanotuña	**Ing. Maritza Badillo**

HALLAZGOS DE AUDITORÍA	
TÍTULO: Los reguladores tipo UPS adjuntados a cada equipo no han sido previamente configurados para que estos provean de energía cuando exista suspensión del servicio eléctrico.	
1. **Condición:** Los reguladores tipo UPS no se ha configurado su batería, ya que estos no cumplen con su función la que es de proveer de energía cuando exista suspensiones de luz.	
2. **Criterio:** No existe un plan de procedimientos para este tipo de actividades.	
3. **Causa**: Poco compromiso en precautelar la seguridad de la información.	
4. **Riesgo:** Perdida de productividad e información importante y necesaria para la institución y usuario.	
5. **Observación:** El nivel de riesgo es Alto	
6. **Recomendación:** Establecer procedimientos para la configuración de las baterías de los UPS o realizar capacitación para el manejo y configuración para este tipo de equipos.	
Responsables:	**Se informa a:**
Egr. Sonia Buñay – Egr. Emilly Guanotuña	**Ing. Maritza Badillo**

HALLAZGOS DE AUDITORÍA
TÍTULO: Espacio Físico del PGI
1. **Condición:** Poco espacio físico
2. **Criterio:** El espacio físico es inadecuado para el número de técnicos que

laboran
3. **Causa:** No se consideró el crecimiento de este Proceso dentro de la Institución.
4. **Riesgo:** Inoperatividad de los Técnicos
5. **Observación:** El nivel de riesgo de que ocurra es Alta
6. **Recomendación:** Readecuar el espacio físico del PGI, ya que este no cuenta con el área física necesaria para este tipo de labor.

Responsables:	**Se informa a:**
Egr. Sonia Buñay – Egr. Emilly Guanotuña	**Ing. Maritza Badillo**

HALLAZGOS DE AUDITORÍA
TÍTULO: Espacio Físico Cuarto de Servidores
1. **Condición:** Poco espacio físico
2. **Criterio:** El espacio físico es inadecuado para el número de servidores y equipos tecnológicos que alberga
3. **Causa:** No se considero el crecimiento de este proceso.
4. **Riesgo:** Inoperatividad en los equipos que se encuentran en esta área
5. **Observación:** El nivel de riesgo de que ocurra es Alta
6. **Recomendación:** Readecuar el espacio físico del cuarto de Servidores para evitar los daños físicos o lógicos ocasionados al maniobrar los equipos.

Responsables:	**Se informa a:**
Egr. Sonia Buñay – Egr. Emilly Guanotuña	**Ing. Maritza Badillo**

HALLAZGOS DE AUDITORÍA
TÍTULO: ESPACIO FISICO PGI
1. **Condición:** Poco espacio físico
2. **Criterio:** El espacio físico es inadecuado para el número de técnicos que laboran

3. **Causa:** No se consideró el crecimiento de este Proceso dentro de la Institución.	
4. **Riesgo:** Inoperatividad de los Técnicos	
5. **Observación:** El nivel de riesgo de que ocurra es Alta	
6. **Recomendación:** Readecuar el espacio físico del PGI, ya que este no cuenta con el área física necesaria para este tipo de labor.	
Responsables:	**Se informa a:**
Egr. Sonia Buñay – Egr. Emilly Guanotuña	**Ing. Maritza Badillo**

FORMULARIO DE VISITAS
Descripción: Cableado de red
Área: PROCESO DE GESTION INFORMATICA
Fecha: 06 - Julio – 2009
Observaciones
El cableado de red en el PGI ha sido instalada de manera provisional
Responsables:
Egr. Sonia Buñay – Egr. Emilly Guanotuña

FORMULARIO DE VISITAS
Descripción: Servidores
Área: CUARTO DE SERVIDORES – PGI
Fecha: 02 – Junio – 2009
Observaciones
Los servidores no todos se cuentan con conexión a un UPS
Los servidores no todos cuentan con Monitores
No se realiza ningún tipo de mantenimiento a estos equipos
No existe etiquetación de los equipos dando facilidad a confusiones
No se realiza limpieza al cuarto de servidores
Sobre los servidores se encuentran cajas de cartón con cables y periféricos en mal estado

Responsables:
Egr. Sonia Buñay – Egr. Emilly Guanotuña

FORMULARIO DE VISITAS
Descripción: Espacio Físico del Proceso de Gestión Informática
Área: PGI
Fecha: 02 – Junio – 2009
Observaciones
Desorden en cada uno de los escritorios de los técnicos, encontrándose sobre éstos, equipos, cajas de cartón, discos duros, CD, herramientas y documentos; ya que los técnicos no cuentan con mobiliario necesario por la falta de espacio
No existe estética en el tendido del cableado eléctrico como del cableado de voz y datos.
No cuenta con un sitio asignado para el mantenimiento de computadoras
Responsables:
Egr. Sonia Buñay – Egr. Emilly Guanotuña

FORMULARIO DE VISITAS
Descripción: DataCenter
Área: CUARTO DE SERVIDORES
Fecha: 02 – Junio - 2009
Observaciones
El manejo del cableado estructurado no es el adecuado ya que existen patch cord mal distribuidos con tamaños poco apropiados, mal ponchados, como también no existe un correcto manejo de colores en los patch cord identificando los de voz y datos.
Los dispositivos de red (hubs, swith,routers) se encuentran en desorden sin ninguna etiquetación.
El rack está conectado a un UPS que no funciona.
Responsables:

Egr. Sonia Buñay – Egr. Emilly Guanotuña

FORMULARIO DE VISITAS
Descripción: Tomas eléctricas
Área: EDIFICIO
Fecha: 06 – Julio – 2009
Observaciones
Los toma corrientes son insuficientes para todos los equipos de cómputo, generando que de una sola toma corriente estén conectados hasta cuatro equipos.
Responsables:
Egr. Sonia Buñay – Egr. Emilly Guanotuña

ANEXO 7.

ENTREVISTAS

- Entrevistas: Fecha: / /

1. ¿Qué recursos se quiere proteger?

   _____

   _____

2. ¿Qué tan importante es el recurso a proteger?

   _____

   _____

3. ¿De qué personas se necesita proteger los recursos?

   _____

   _____

4. ¿A qué amenazas cree usted que se encuentra expuesta la institución y que tan reales son?

   _____

   _____

---------- **----------**

Egr. Sonia Buñay **Egr. Emilly Guanotuña**

Ing. Maritza Badillo

Coordinadora del Proceso

- Entrevistas: Fecha: / /

1. Se realiza mantenimiento a los computadores desktop?

---

2. Se realiza mantenimiento a los periféricos?

---

3. Se realiza mantenimiento a los servidores?

---

4. Se realiza mantenimientos a los equipos de comunicación?

---

5. Con que periodicidad se realiza el mantenimiento de:?
   Computadores:
   Periféricos:
   Servidores:
   Equipos de Comunicación:
6. Quien realiza el mantenimiento?

---

7. Qué Proceso organiza y efectúa el mantenimiento de los equipos de computación, periféricos, servidores y equipos de comunicación?

---------- **----------**

Egr. Sonia Buñay **Egr. Emilly Guanotuña**

Ing. Maritza Badillo

Coordinadora del Proceso

ANEXO 8.

MONITOREO DE LA RED EN LA DPSP

SOFTWARE:

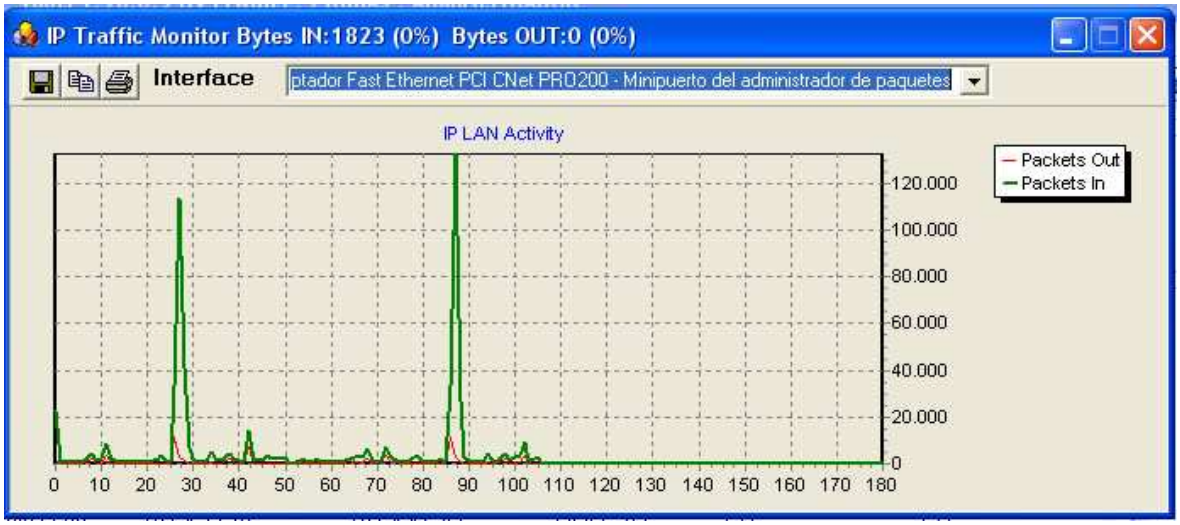
IP TOOLS 1.98.0.9 BY Erwan L. /RunAs (CABLEADA)

NET STUMBLER(INALAMBRICA)

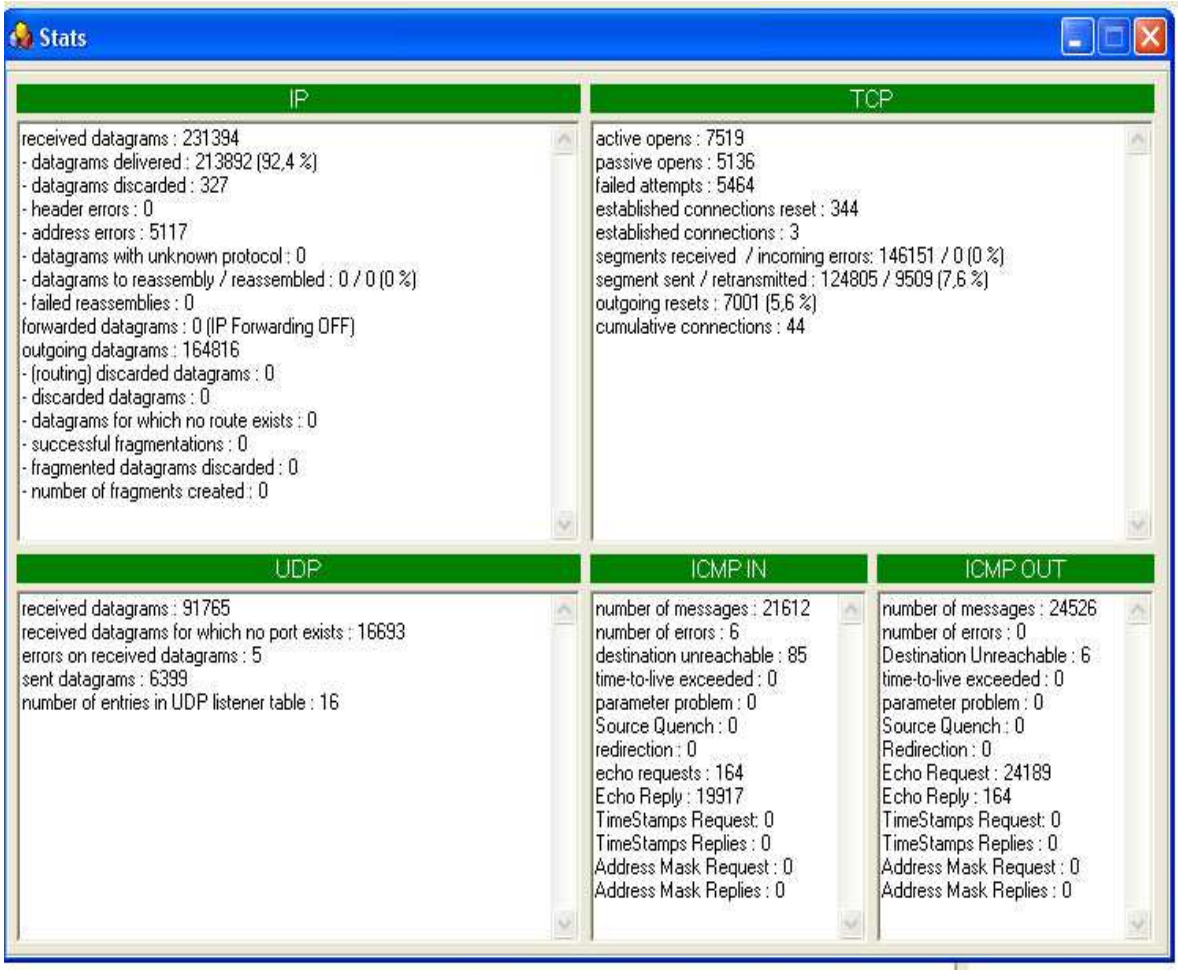
TESTEO DE LA RED(COMANDO NETSTAT)

RED CABLEADA

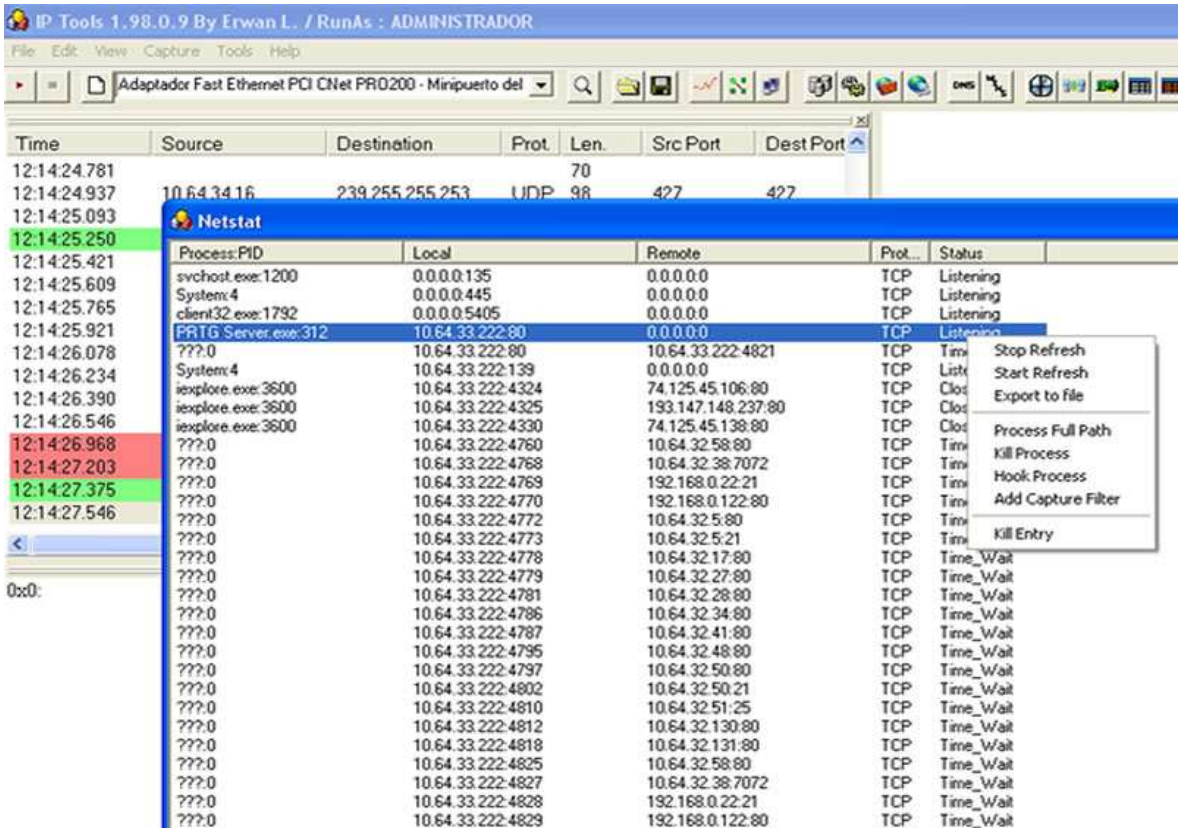
Monitoreo del Ancho de Banda



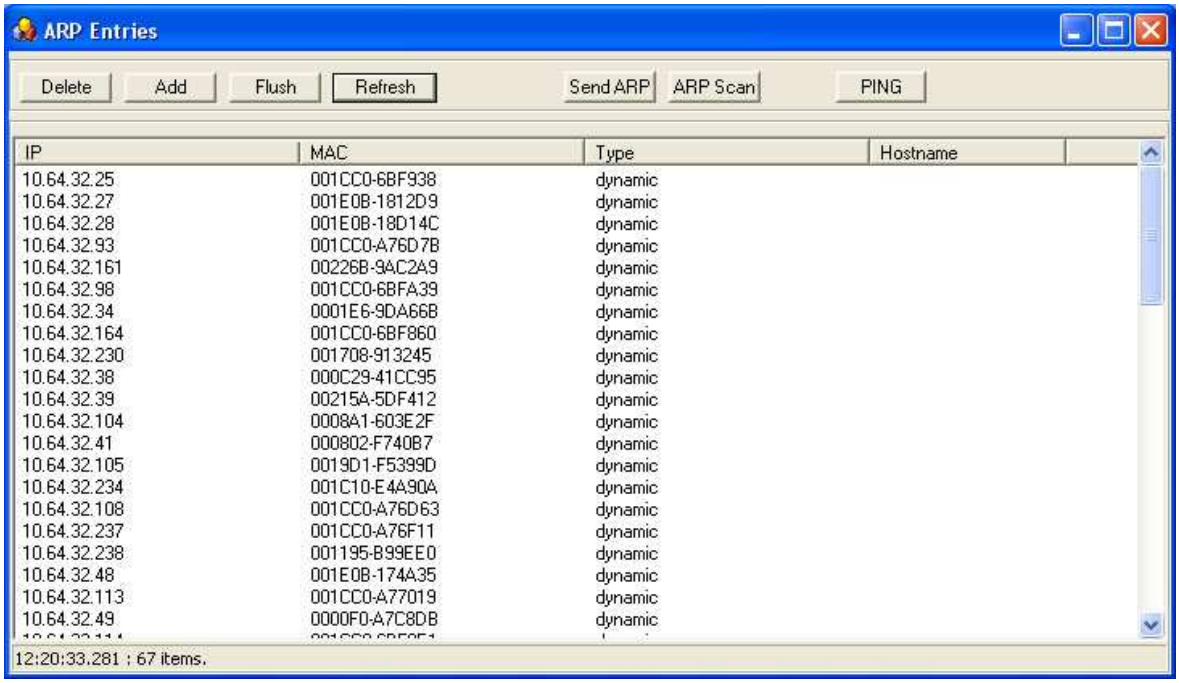
Estadística de los Adaptadores



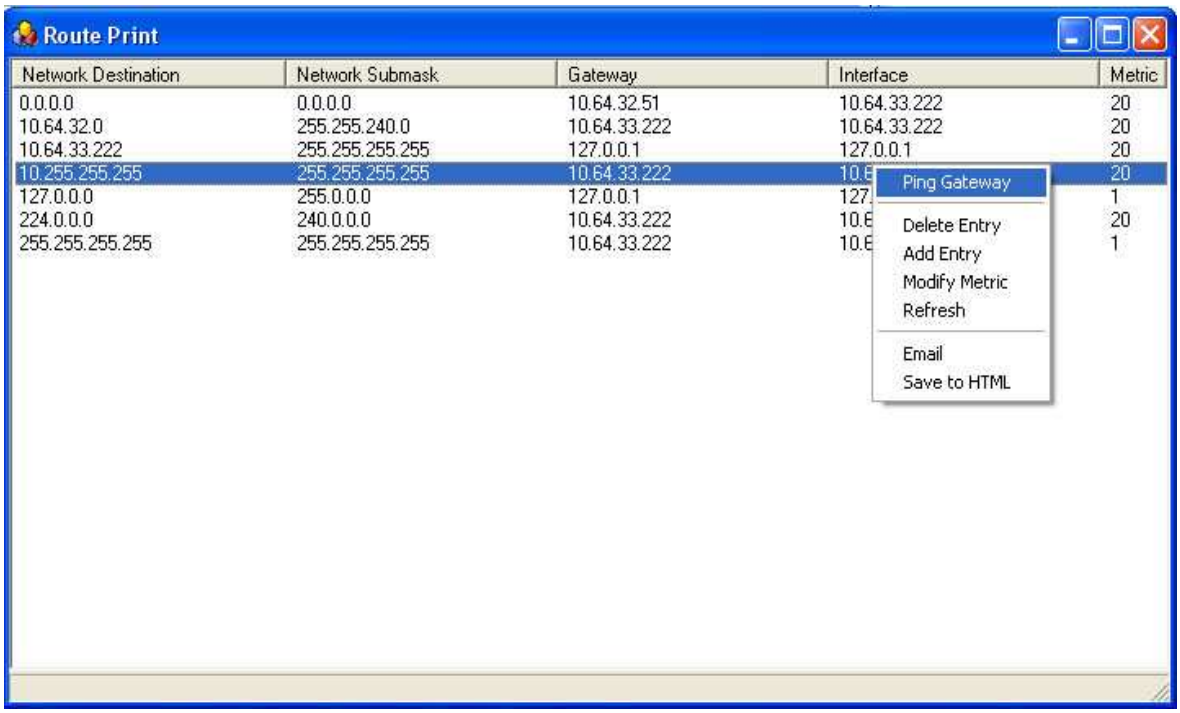
Listado y Gestión de los Puertos Abiertos



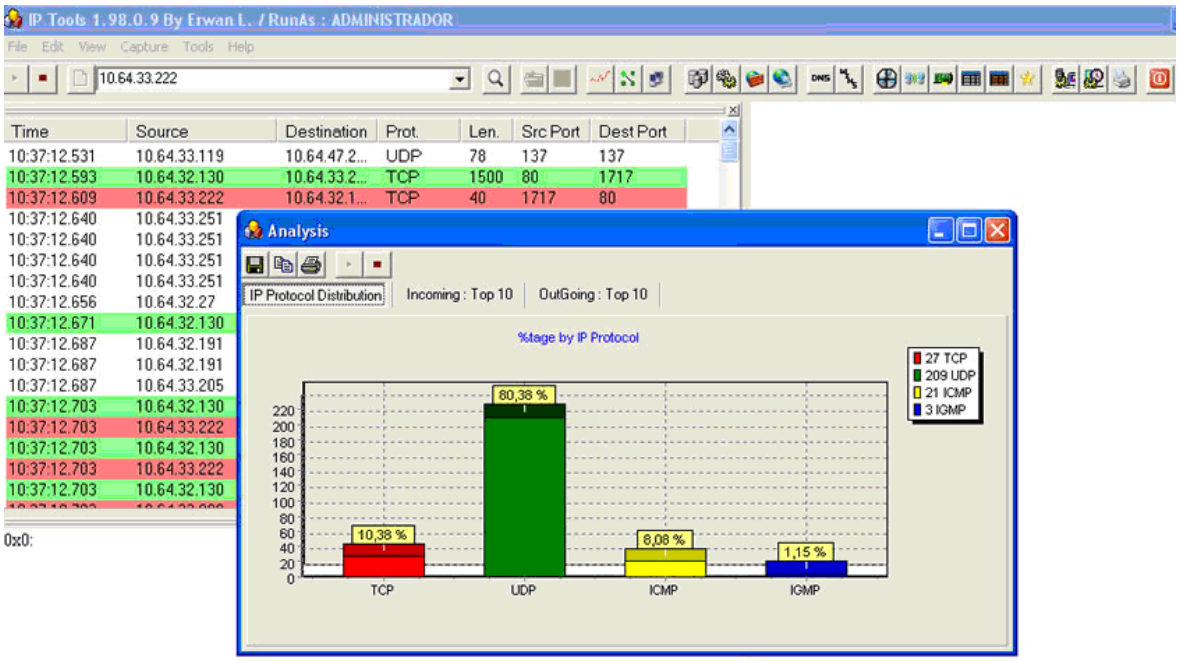
Conociendo la dirección MAC con su respectiva dirección IP



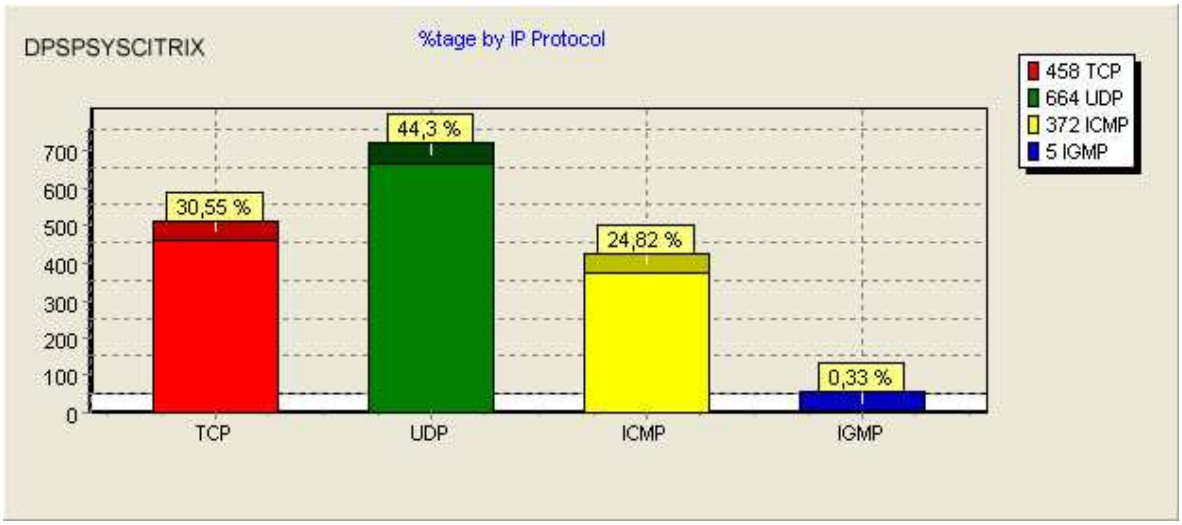
Lista y Gestión de rutas



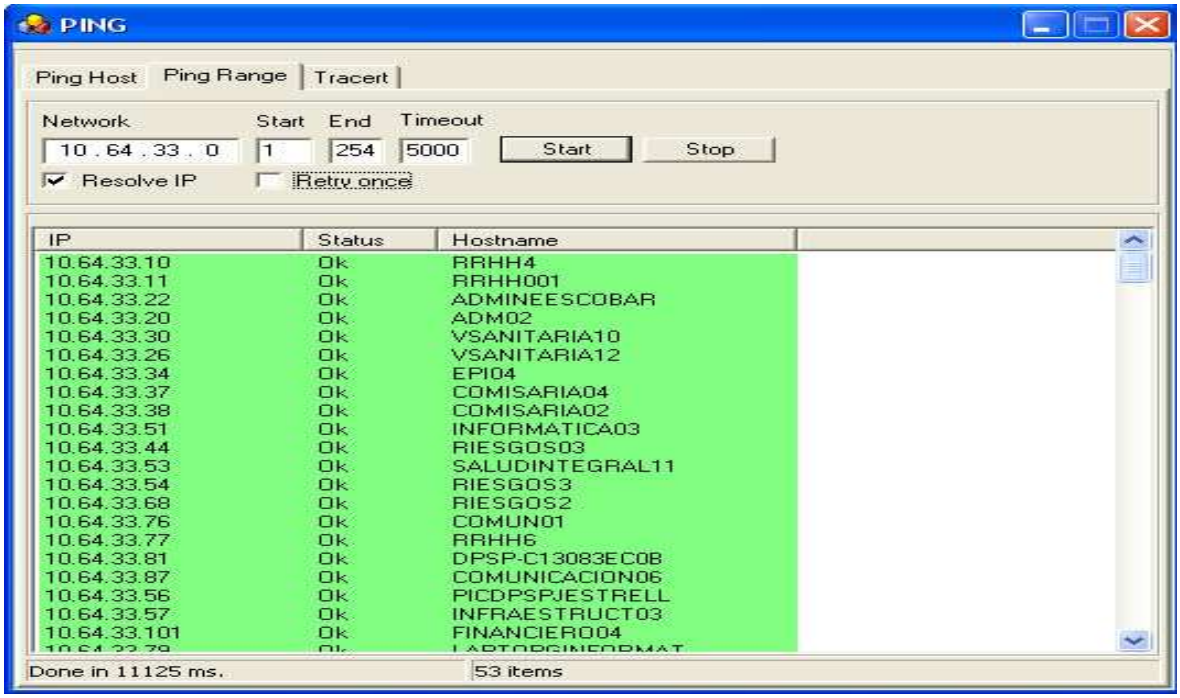
Análisis a los puertos más utilizados de la red



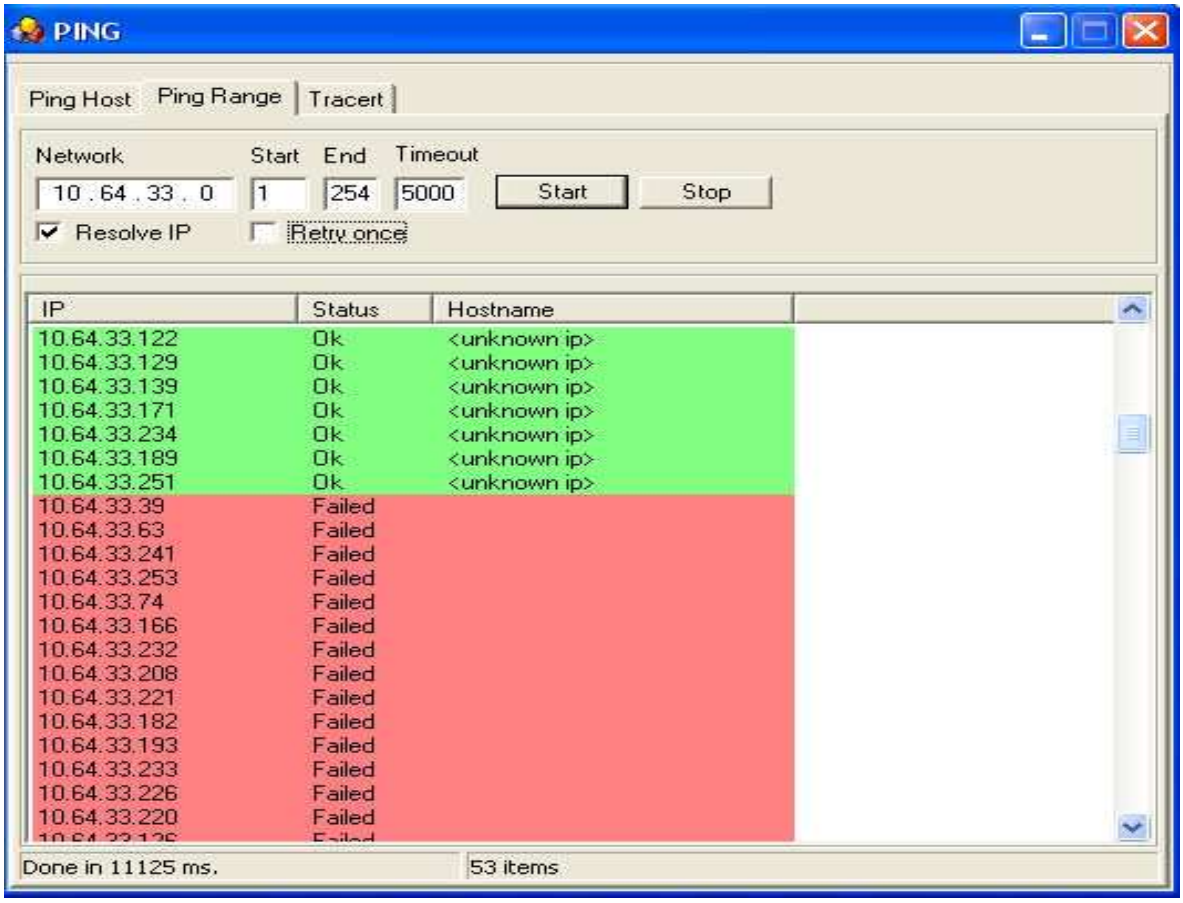
Análisis realizado al Servidor DPSPSYCITRIX



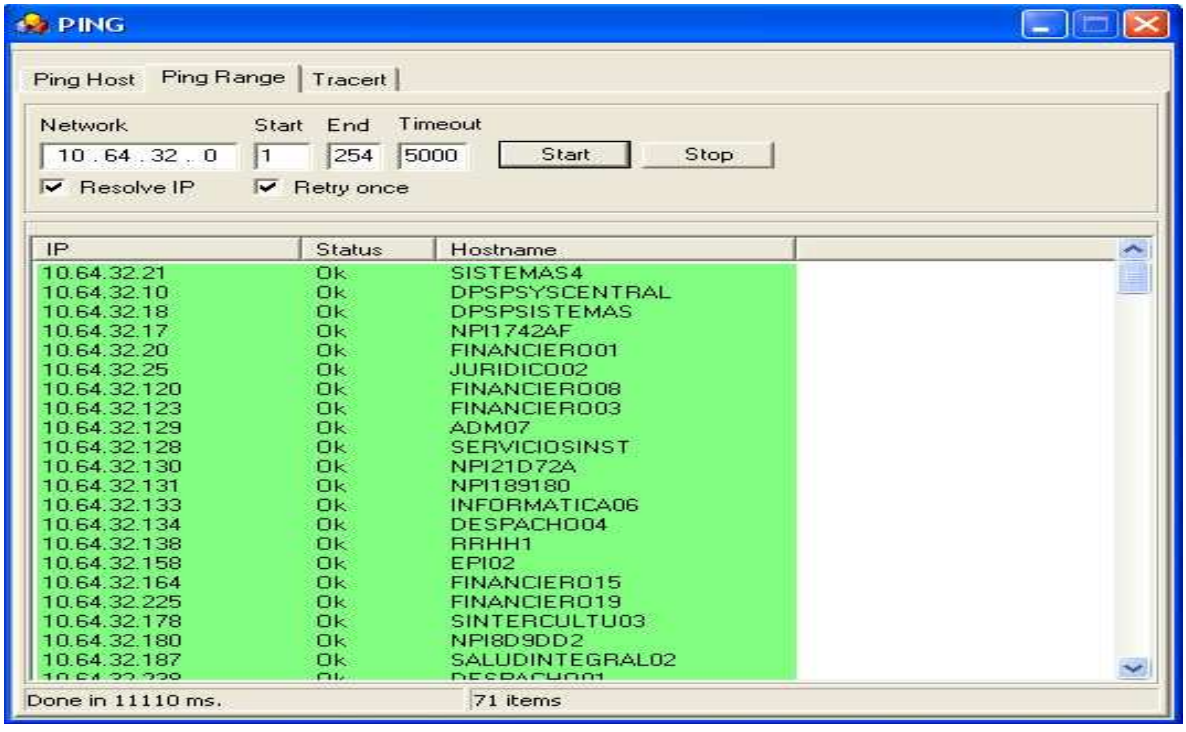
Listado de Equipos conectados de la red 10.64.33.0



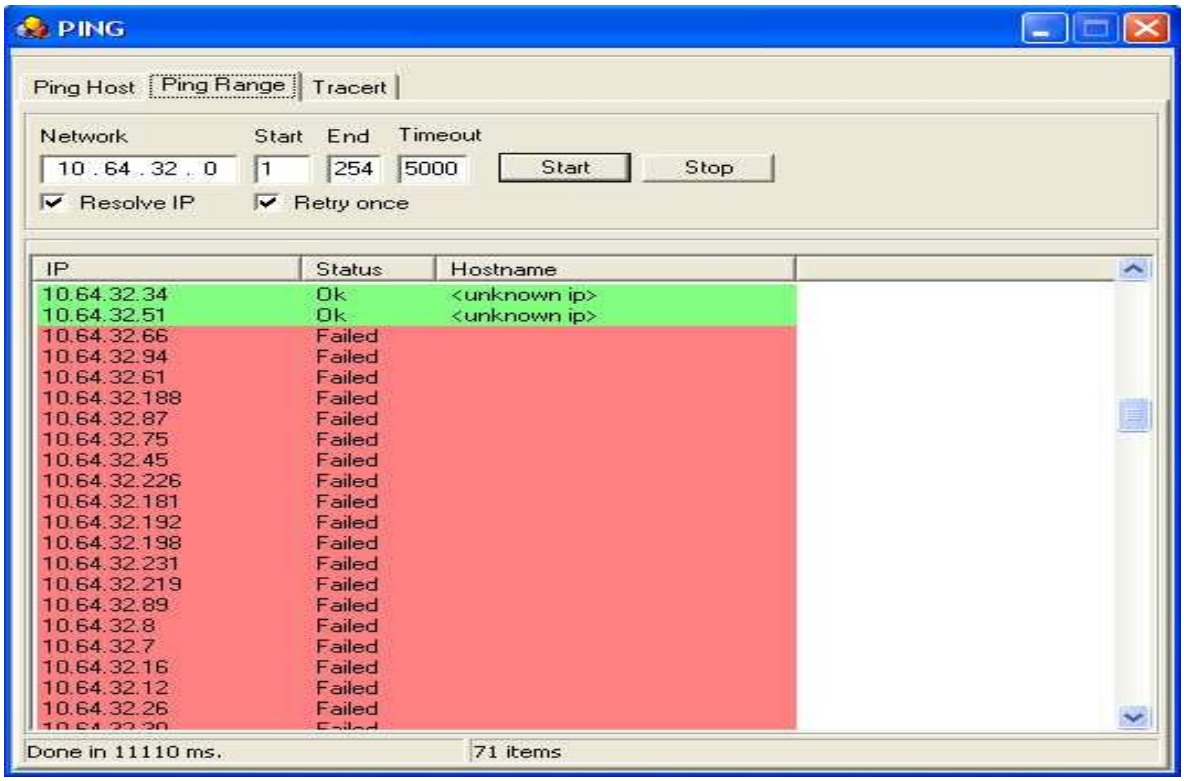
Listado de Equipos conectados y desconectados de la red 10.64.33.0



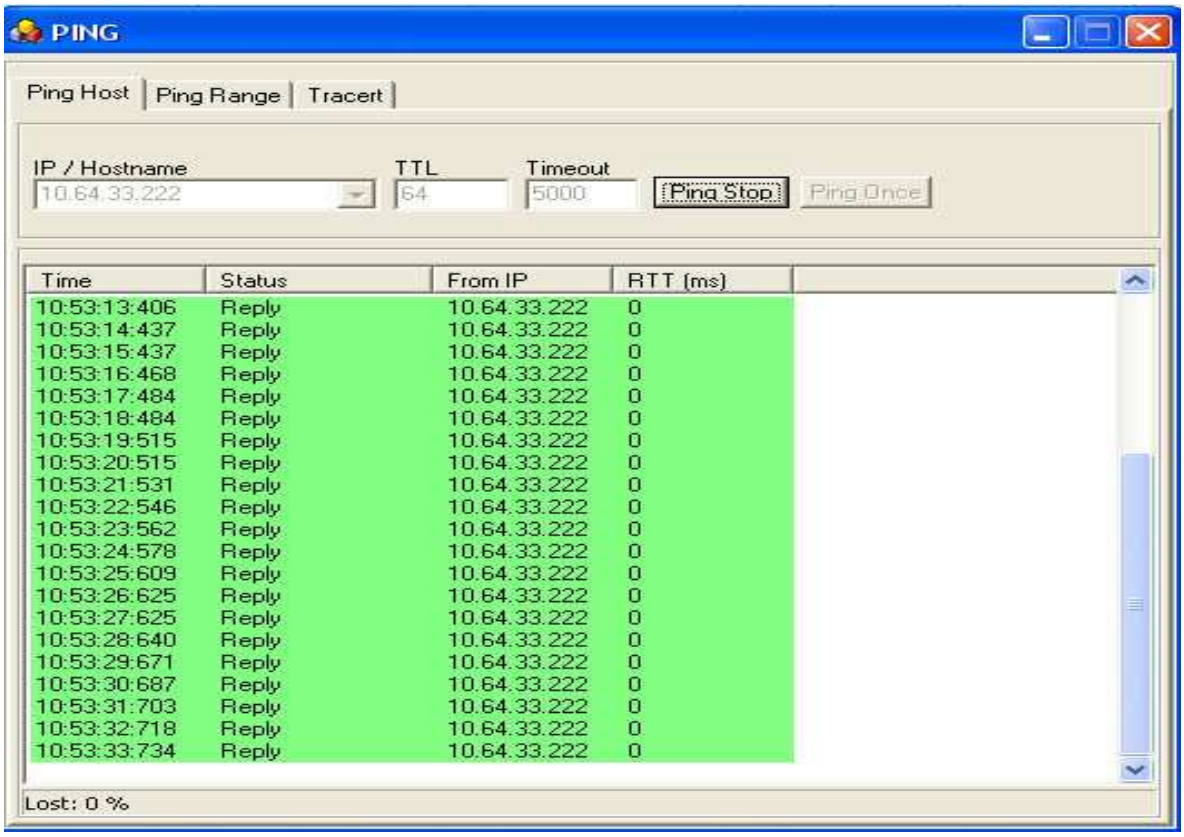
Listado de Equipos conectados de la red 10.64.32.0



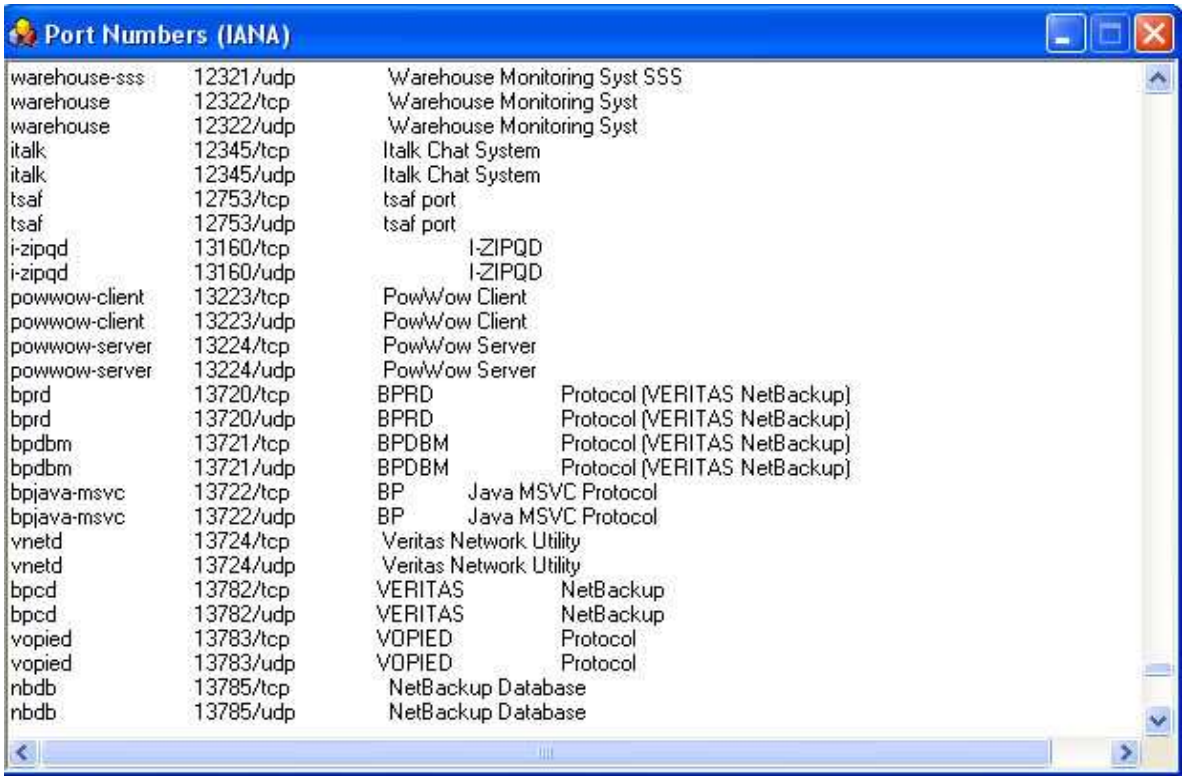
Listado de Equipos conectados y desconectados de la red 10.64.32.0



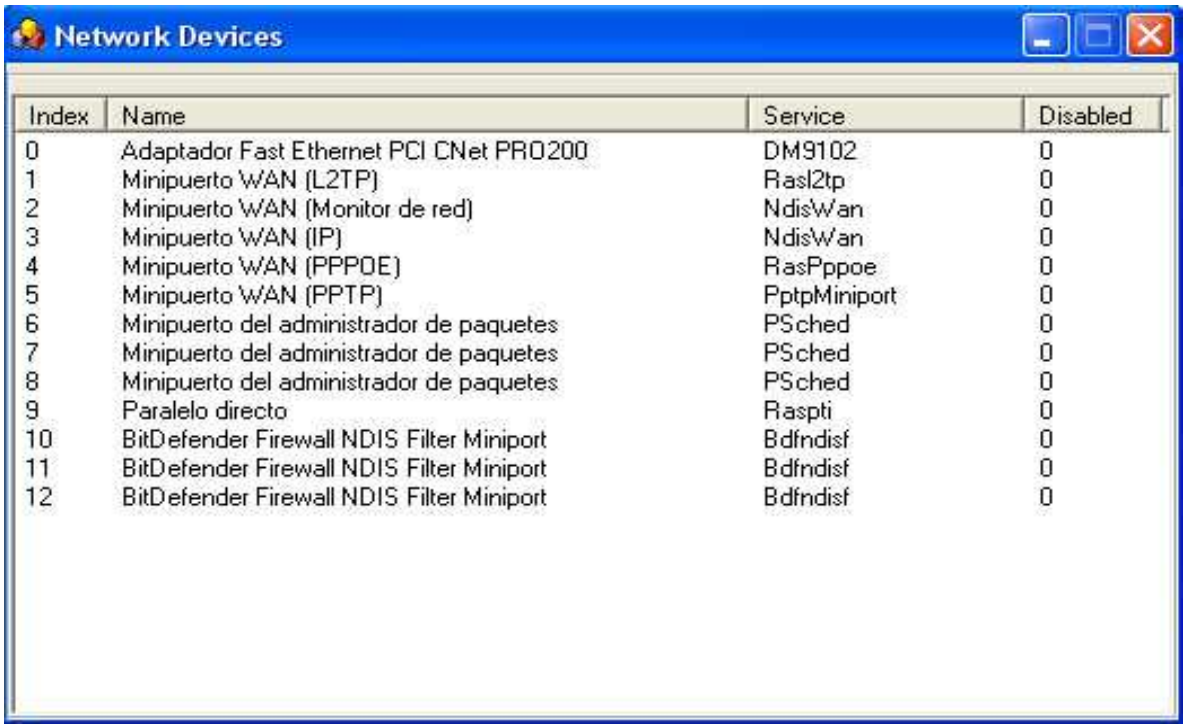
Listado Host con respuesta



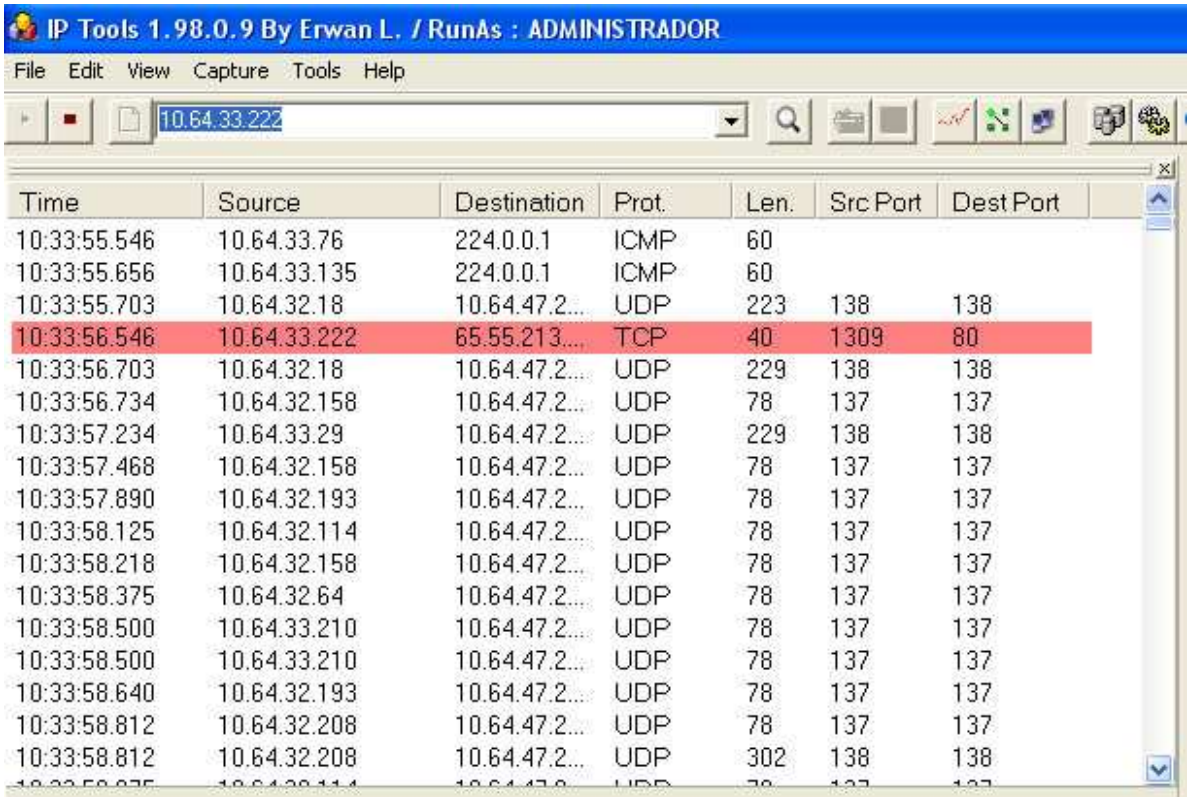
Puertos



Dispositivos de Red

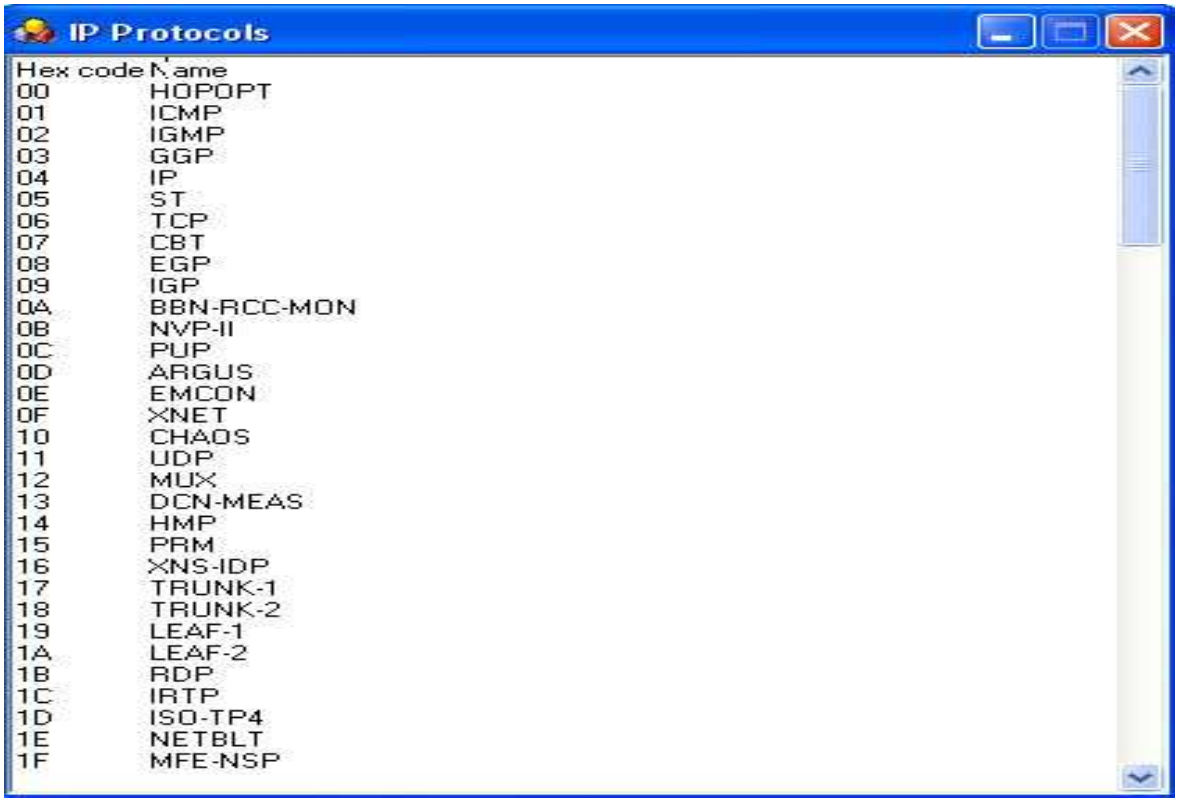


Listado de los Equipos conectados en la red con el Protocolo y Puerto que utilizan



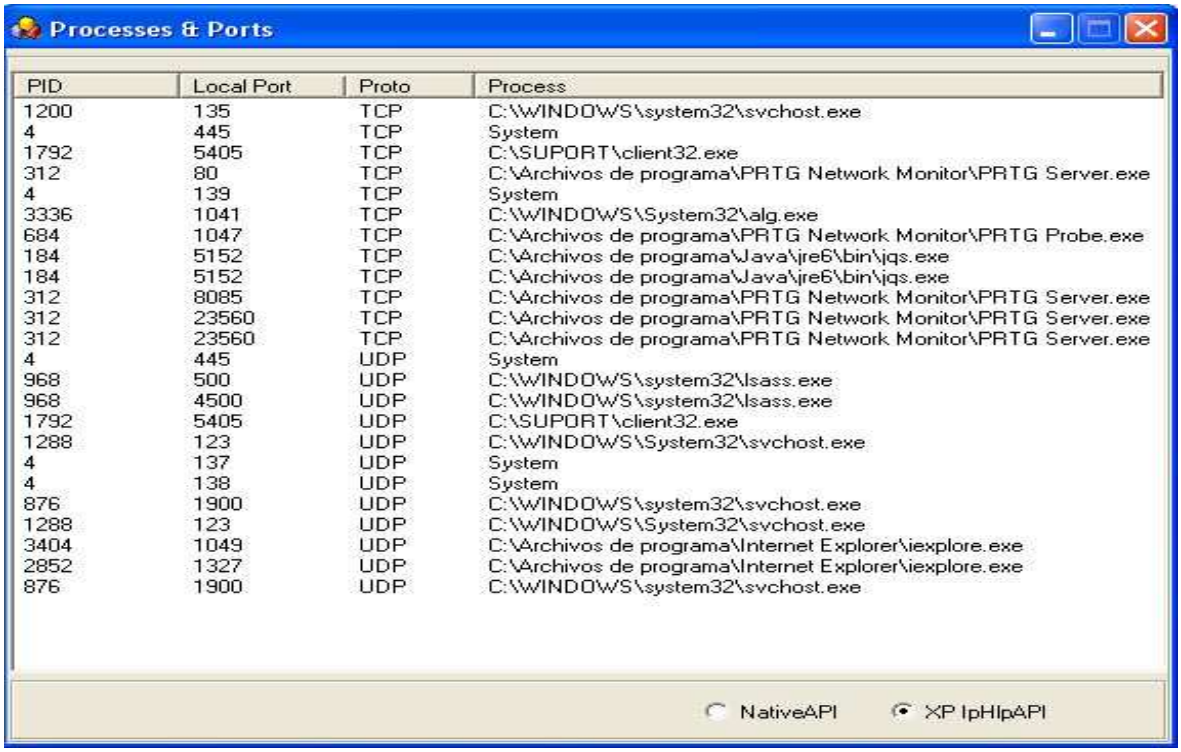
Time	Source	Destination	Prot.	Len.	Src Port	Dest Port
10:33:55.546	10.64.33.76	224.0.0.1	ICMP	60		
10:33:55.656	10.64.33.135	224.0.0.1	ICMP	60		
10:33:55.703	10.64.32.18	10.64.47.2...	UDP	223	138	138
10:33:56.546	10.64.33.222	65.55.213....	TCP	40	1309	80
10:33:56.703	10.64.32.18	10.64.47.2...	UDP	229	138	138
10:33:56.734	10.64.32.158	10.64.47.2...	UDP	78	137	137
10:33:57.234	10.64.33.29	10.64.47.2...	UDP	229	138	138
10:33:57.468	10.64.32.158	10.64.47.2...	UDP	78	137	137
10:33:57.890	10.64.32.193	10.64.47.2...	UDP	78	137	137
10:33:58.125	10.64.32.114	10.64.47.2...	UDP	78	137	137
10:33:58.218	10.64.32.158	10.64.47.2...	UDP	78	137	137
10:33:58.375	10.64.32.64	10.64.47.2...	UDP	78	137	137
10:33:58.500	10.64.33.210	10.64.47.2...	UDP	78	137	137
10:33:58.500	10.64.33.210	10.64.47.2...	UDP	78	137	137
10:33:58.640	10.64.32.193	10.64.47.2...	UDP	78	137	137
10:33:58.812	10.64.32.208	10.64.47.2...	UDP	78	137	137
10:33:58.812	10.64.32.208	10.64.47.2...	UDP	302	138	138

Protocolos Disponibles

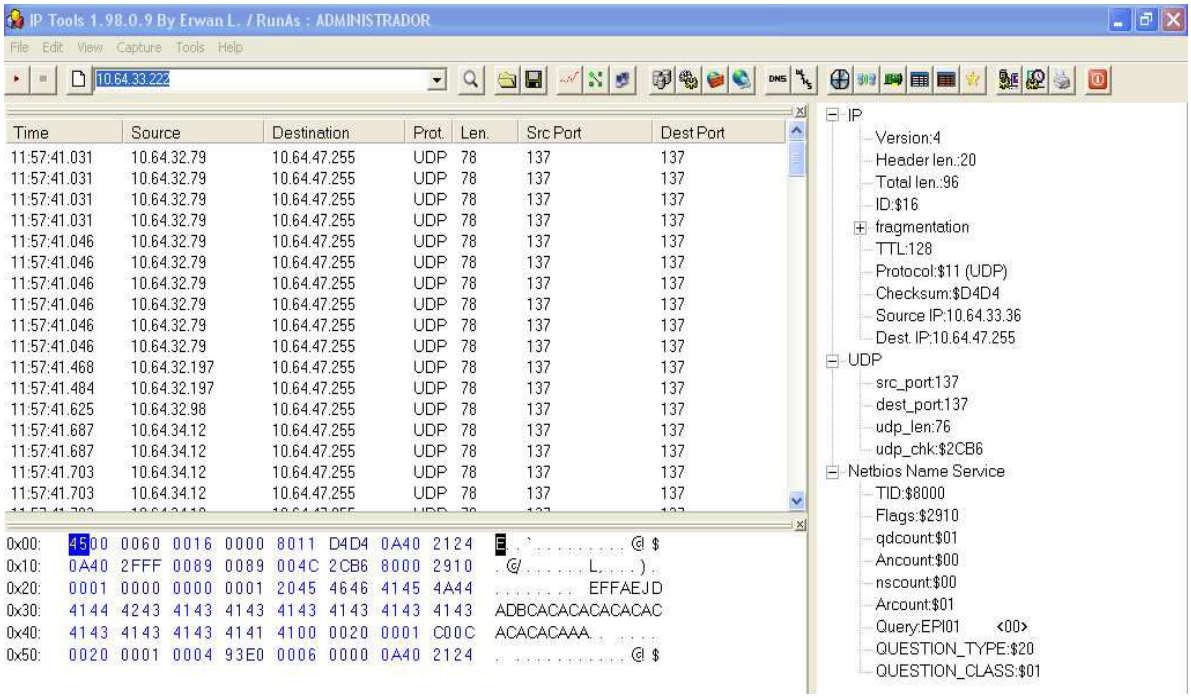


Hex code	Name
00	HOPOPT
01	ICMP
02	IGMP
03	GGP
04	IP
05	ST
06	TCP
07	CBT
08	EGP
09	IGP
0A	BBN-RCC-MON
0B	NVP-II
0C	PUP
0D	ARGUS
0E	EMCON
0F	XNET
10	CHAOS
11	UDP
12	MUX
13	DCN-MEAS
14	HMP
15	PRM
16	XNS-IDP
17	TRUNK-1
18	TRUNK-2
19	LEAF-1
1A	LEAF-2
1B	RDP
1C	IRTP
1D	ISO-TP4
1E	NETBLT
1F	MFE-NSP

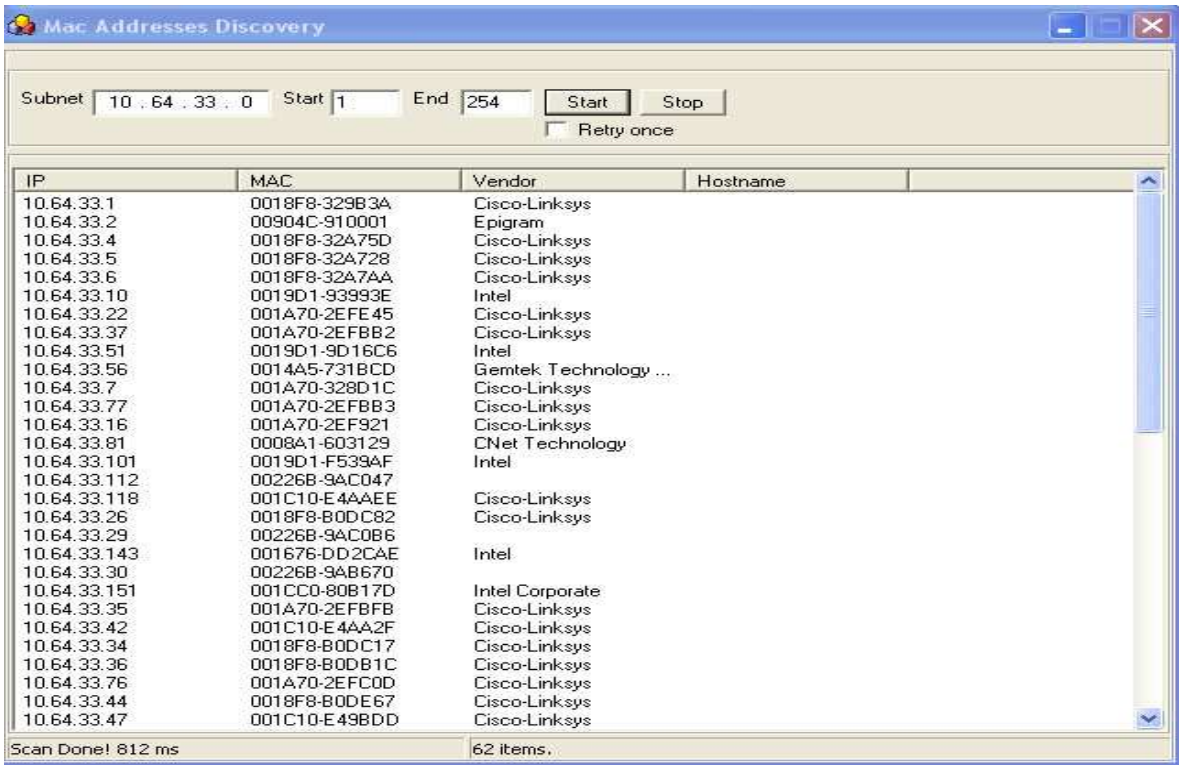
Procesos y Puertos



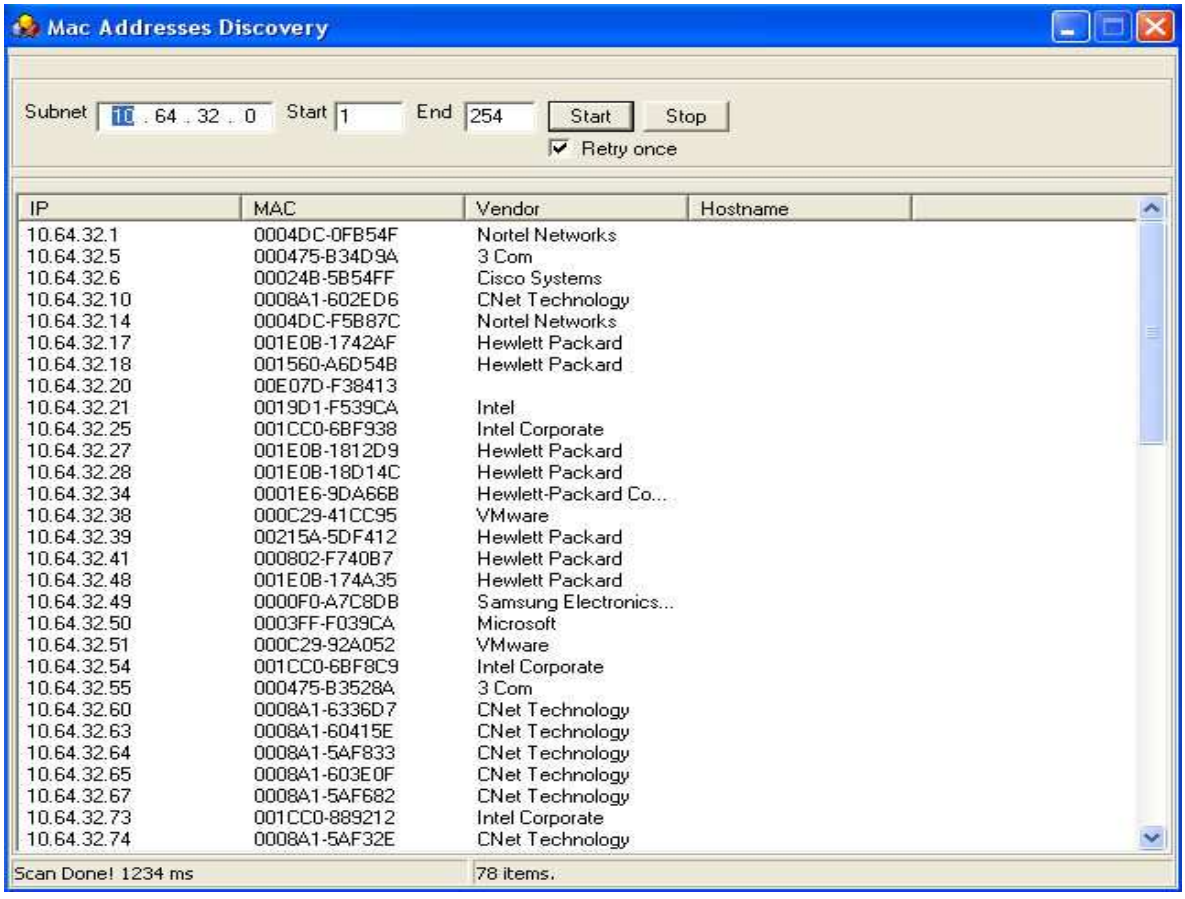
Capturado Modo Winpcap



Listado de Direcciones Mac Red 10.64.33.0

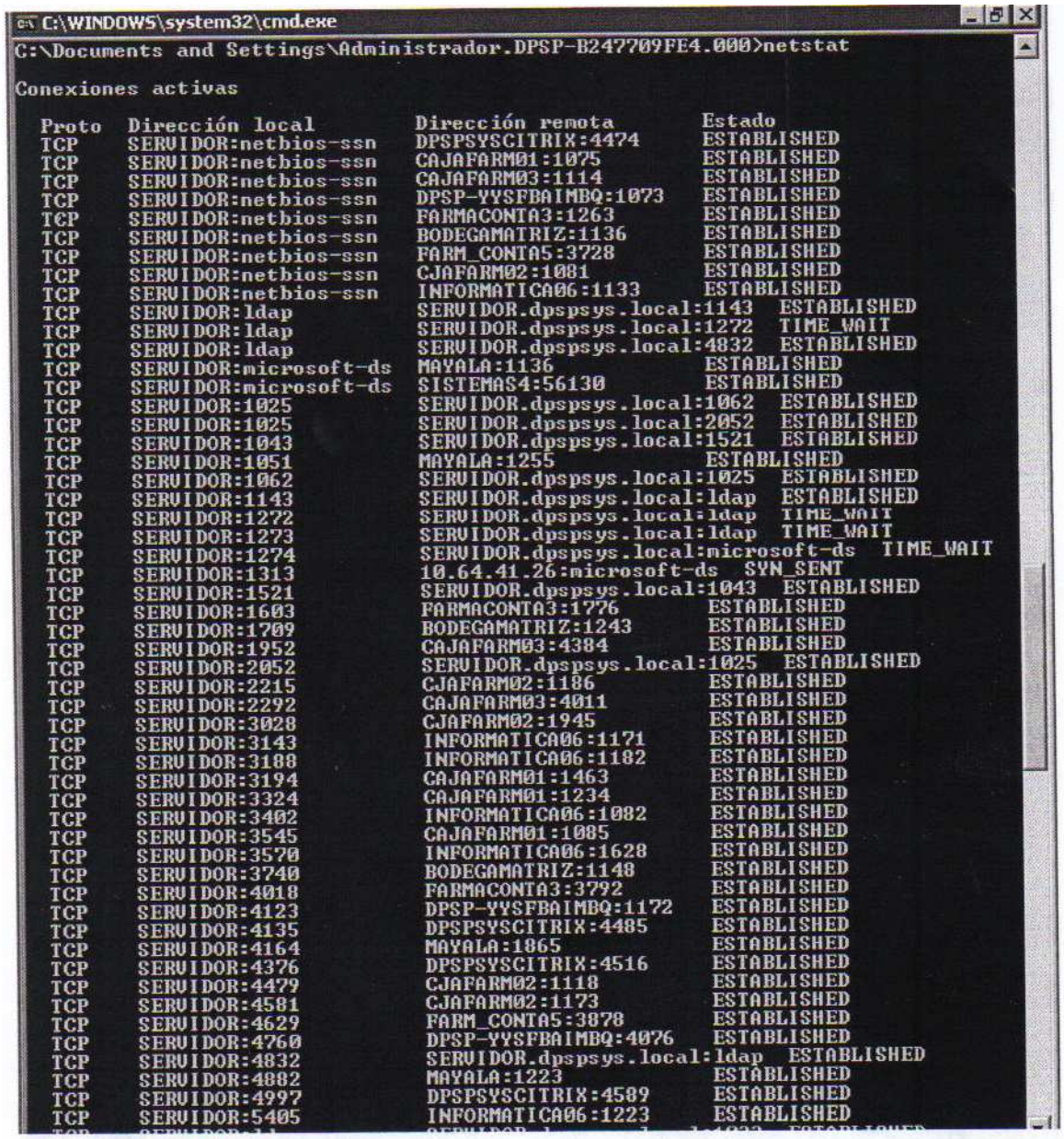


LISTADO DE DIRECCIONES MAC RED 10.64.32.0



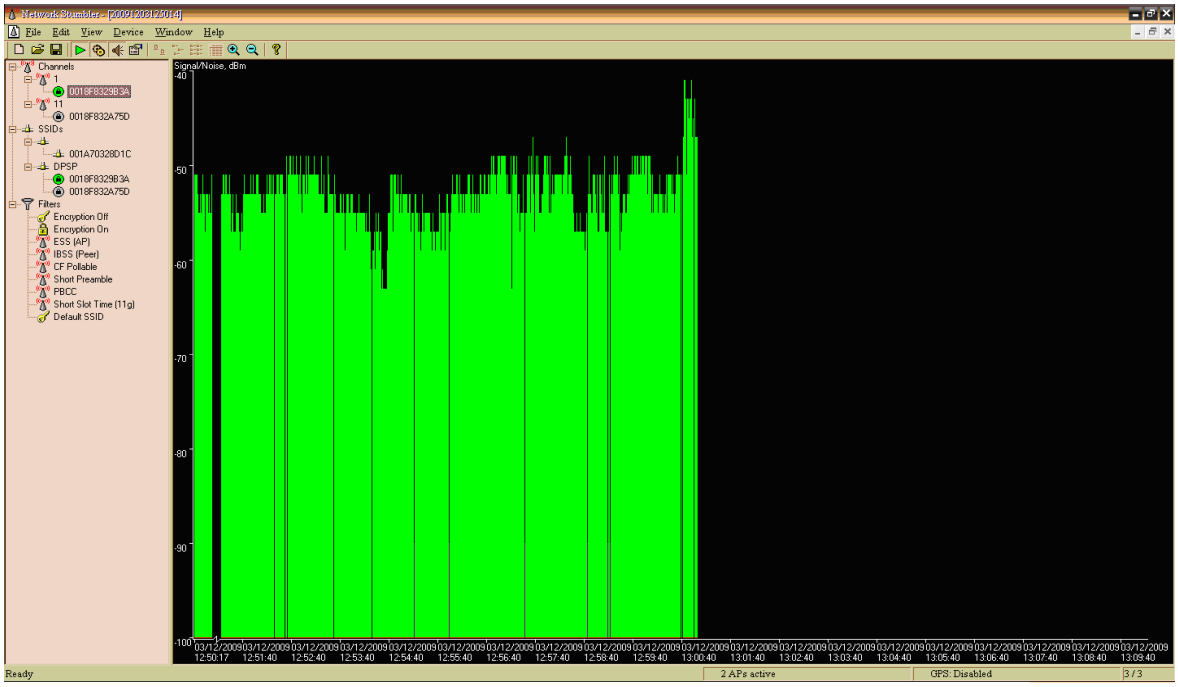
Testeo de la Red-Comando Netstat

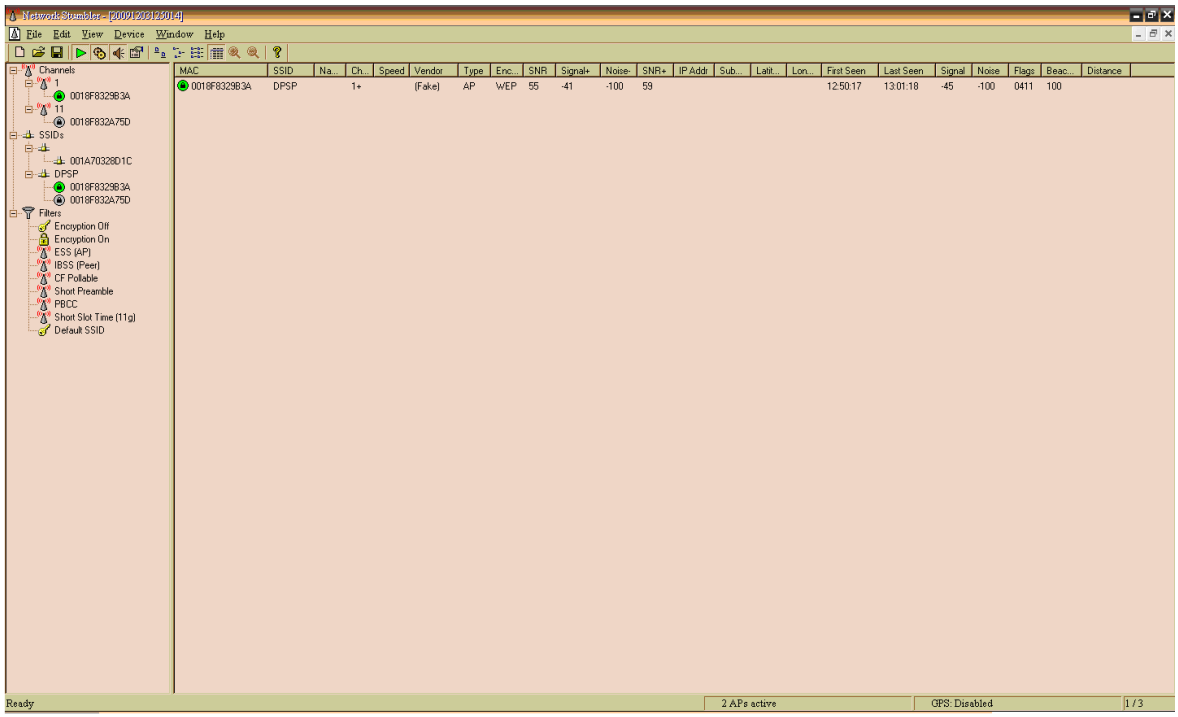
Nombre del servidor : SERVIDOR

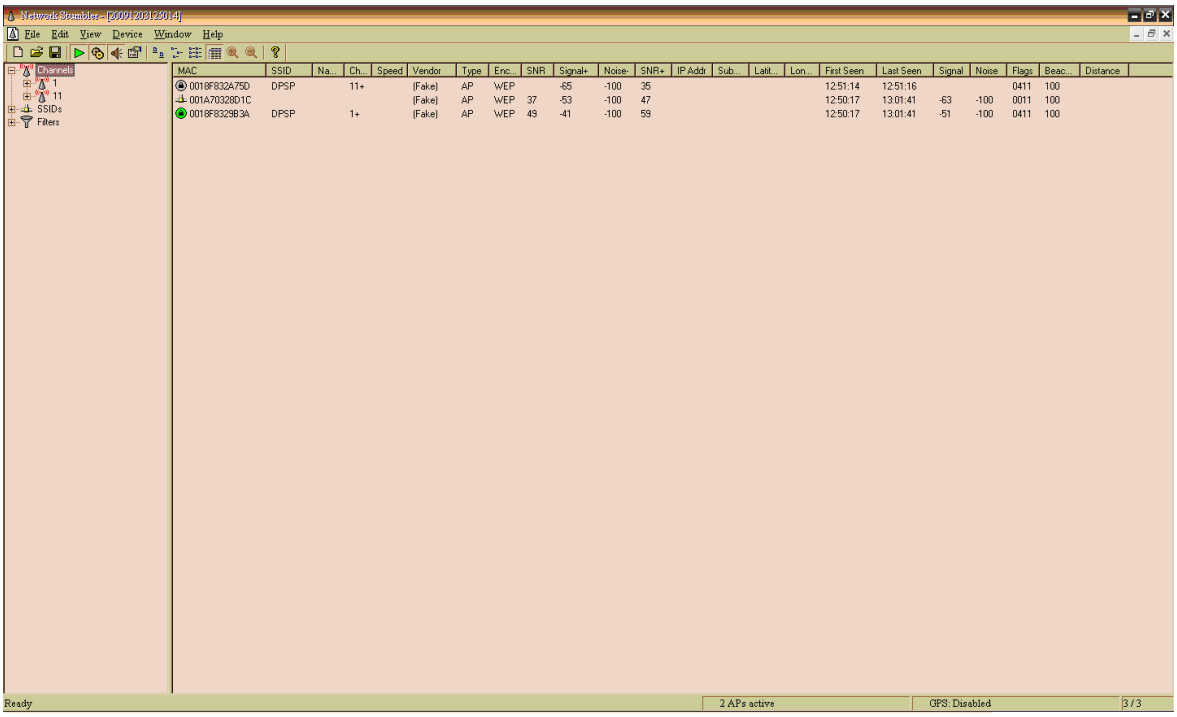


RED INALÁMBRICA

Monitoreo

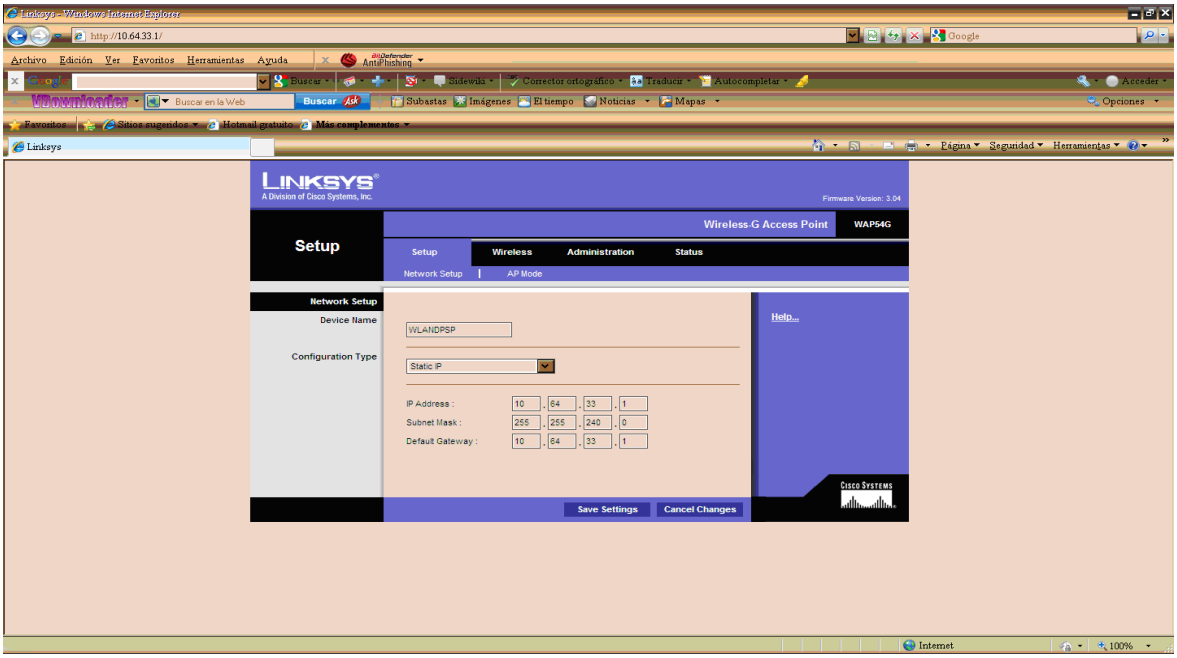

Network Stumbler - [2009120312014]
File Edit View Device Window Help
Channels
1
0018F8329B3A
11
0018F832A75D
SSIDs
001A70328D1C
DPSP
0018F8329B3A
0018F832A75D
Filters
Encryption Off
Encryption On
ESS (AP)
IBSS (Peer)
CF Pollable
Short Preamble
PBCC
Short Slot Time (11g)
Default SSID
Signal/Noise, dBm
-40
-50
-60
-70
-80
-90
-100
03/12/2009 12:50:17
03/12/2009 12:51:40
03/12/2009 12:52:40
03/12/2009 12:53:40
03/12/2009 12:54:40
03/12/2009 12:55:40
03/12/2009 12:56:40
03/12/2009 12:57:40
03/12/2009 12:58:40
03/12/2009 12:59:40
03/12/2009 13:00:40
03/12/2009 13:01:40
03/12/2009 13:02:40
03/12/2009 13:03:40
03/12/2009 13:04:40
03/12/2009 13:05:40
03/12/2009 13:06:40
03/12/2009 13:07:40
03/12/2009 13:08:40
03/12/2009 13:08:40
Ready
2 APs active
GPS: Disabled
3 / 3

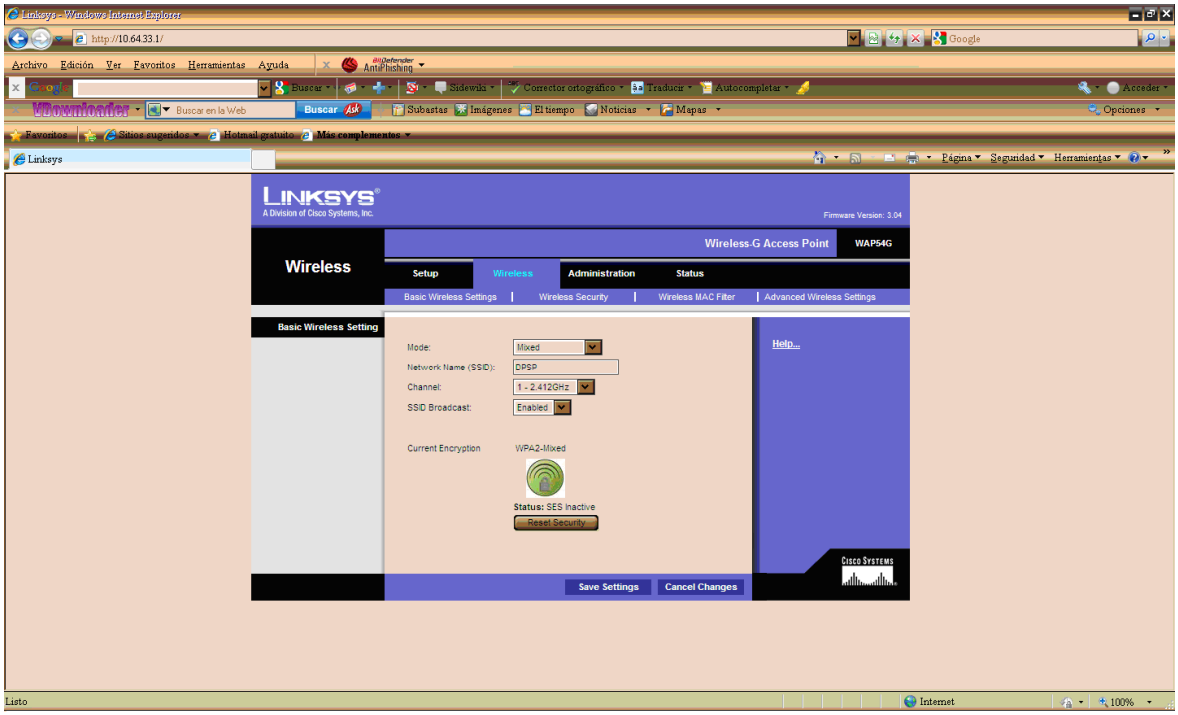

Network Stumbler - [2009120312014]
File Edit View Device Window Help
Channels
1
0018F8329B3A
11
0018F832A75D
SSIDs
001A70328D1C
DPSP
0018F8329B3A
0018F832A75D
Filters
Encryption Off
Encryption On
ESS (AP)
IBSS (Peer)
CF Pollable
Short Preamble
PBCC
Short Slot Time (11g)
Default SSID
MAC SSID Na... Ch... Speed Vendor Type Enc... SNR Signal+ Noise- SNR+ IP Addr Sub... Latit... Lon... First Seen Last Seen Signal Noise Flags Beac... Distance
0018F8329B3A DPSP 1+ (Fake) AP WEP 55 -41 -100 59 12:50:17 13:01:18 -45 -100 0411 100
Ready
2 APs active
GPS: Disabled
1 / 3

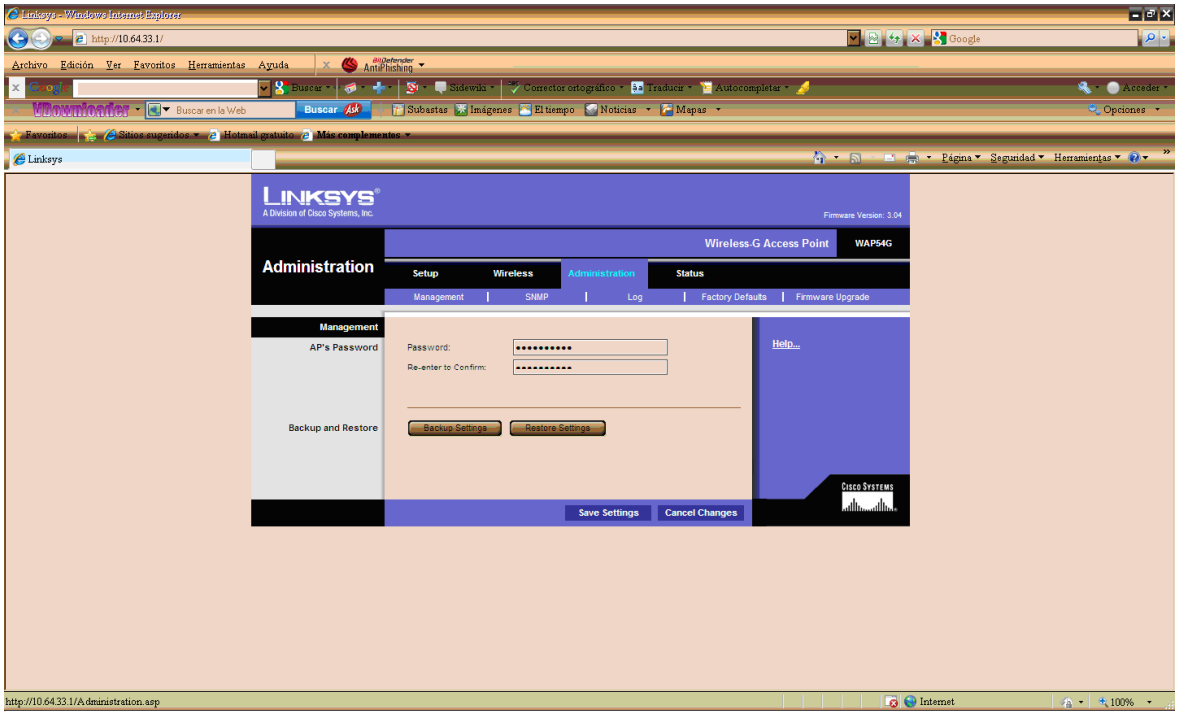


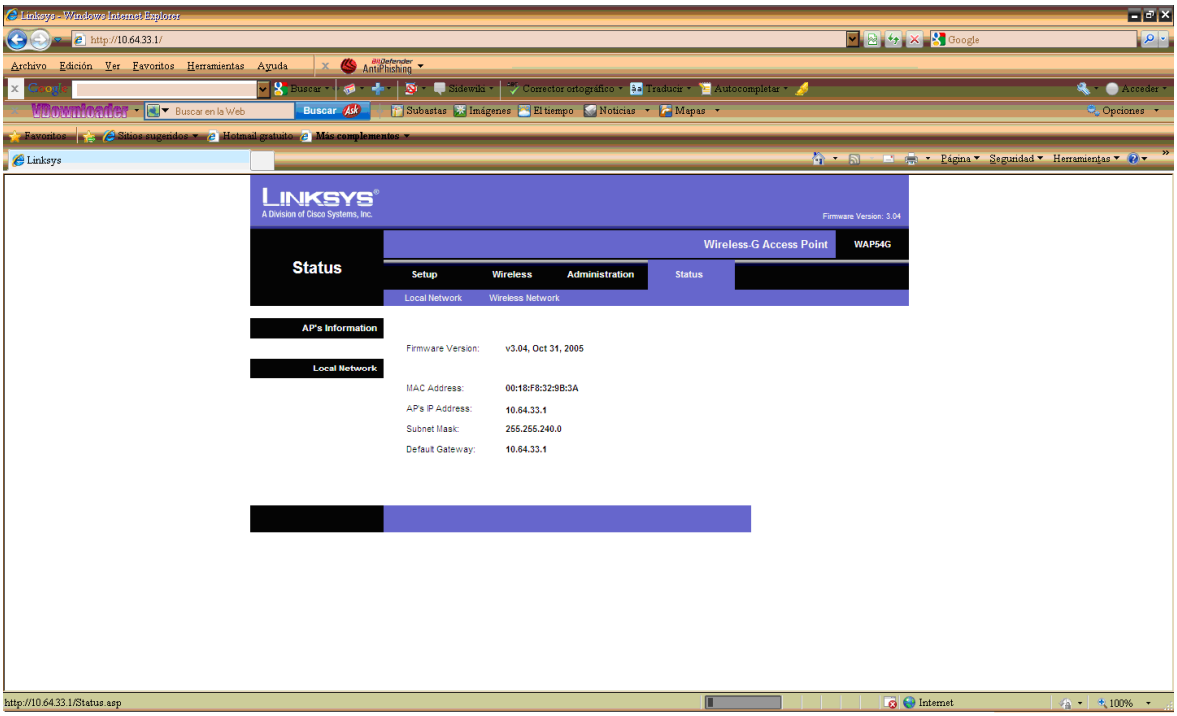
Configuración de los Access Point

En las siguientes figuras se muestra la configuración de los Access Point mediante el browser.




Linksys - Windows Internet Explorer
http://10.64.33.1/
LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: 3.04
Wireless-G Access Point
WAP54G
Wireless
Setup
Wireless
Administration
Status
Basic Wireless Settings
Wireless Security
Wireless MAC Filter
Advanced Wireless Settings
Basic Wireless Setting
Mode:
Mixed
Network Name (SSID):
DPSP
Channel:
1 - 2.412GHz
SSID Broadcast:
Enabled
Current Encryption
WPA2-Mixed
Status: SES Inactive
Reset Security
Help...
Save Settings
Cancel Changes
Listo
Internet
100%


Linksys - Windows Internet Explorer
http://10.64.33.1/
LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: 3.04
Wireless-G Access Point
WAP54G
Administration
Setup
Wireless
Administration
Status
Management
SNMP
Log
Factory Defaults
Firmware Upgrade
Management
AP's Password
Password:
Re-enter to Confirm:
Backup and Restore
Backup Settings
Restore Settings
Help...
Save Settings
Cancel Changes
http://10.64.33.1/Administration.asp
Internet
100%

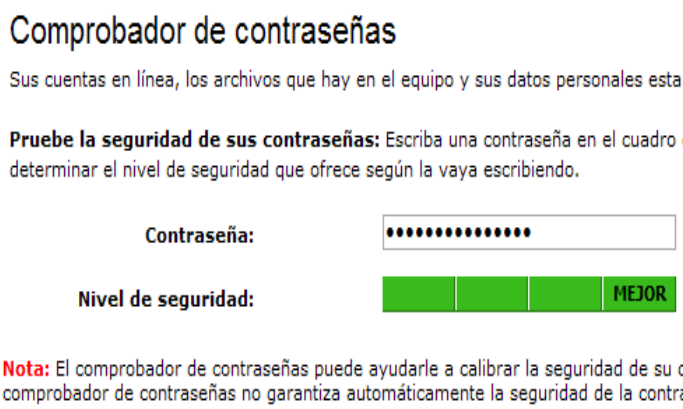

Linksys - Windows Internet Explorer
http://10.64.33.1/
Archivo Edición Ver Favoritos Herramientas Ayuda
Linksys
LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: 3.04
Wireless-G Access Point
WAP54G
Status
Setup
Wireless
Administration
Status
Local Network
Wireless Network
AP's Information
Firmware Version:
v3.04, Oct 31, 2005
Local Network
MAC Address:
00:18:F8:32:9B:3A
AP's IP Address:
10.64.33.1
Subnet Mask:
255.255.240.0
Default Gateway:
10.64.33.1
http://10.64.33.1/Status.asp
Internet
100%

ANEXO 09.

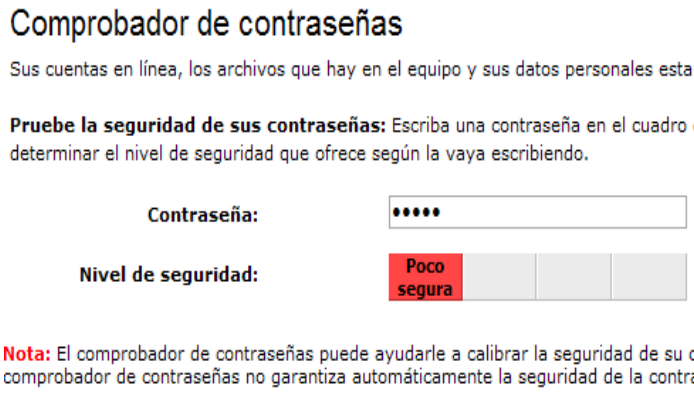
COMPROBADOR DE SEGURIDAD EN PASSWORDS

Comprobación del Nivel de Seguridad de los password asignados a los usuarios de la DPSP y password del usuario Administrador

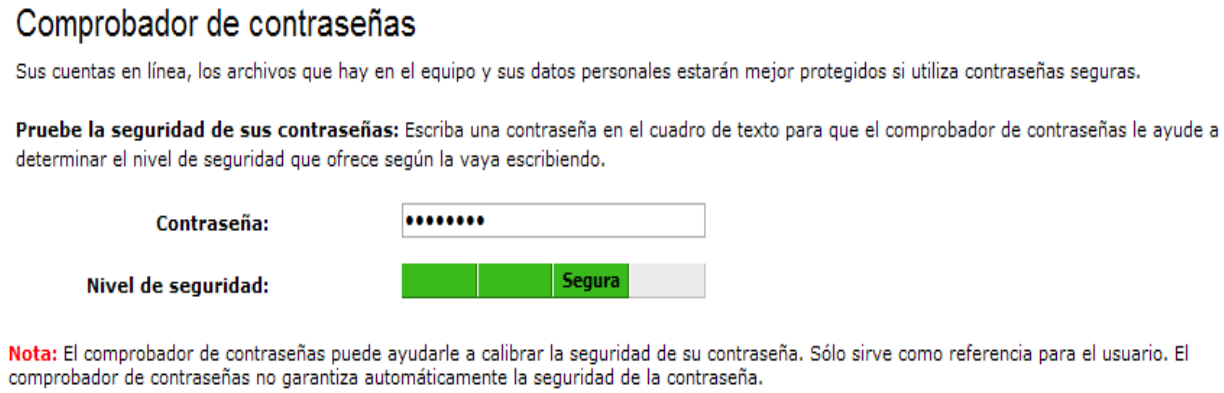
- **PASSWORD:** Administrador



- **PASSWORD:** Usuario de correo electrónico



- **PASSWORD:** Usuario de estaciones de trabajo.



ANEXO 10.

CERTIFICACIÓN DE CABLEADO

EQUIPO FLUKE DTX 1800(UTP)